

Mobile Identity
UK Research Summary

June 2013

Restricted - Confidential Information
© GSM Association 2013
All GSMA meetings are conducted in full compliance with the GSMA's anti-trust compliance policy

Objective: provide an integrated view of the UK market with respect to digital / mobile identity

- An integrated view from consumers, industry experts and service providers on the **opportunities and challenges** with respect to mobile identity
- What are the **needs, current pain points and demand** from consumers and service providers for mobile identity
- What are the current and future **use cases** for the implementation of mobile identity solutions
- What is the **business model** for taking this to market and what are the perceptions of potential providers



Research conducted in accordance with ISO 20252

Research approach and scope

Subject Matter Experts Depth Interviews



30 telephone interviews

With independent consultants, ID experts and architects, innovation or strategic functions in major telecoms and technology companies

Service Provider Depth Interviews



30 telephone interviews

Approximately half with major banks, retailers, sites and service providers to government

Other half with smaller less well known service providers

Consumer Focus Groups



8 focus groups

With 8 respondents each, lasting 90 minutes per group

Conducted 2 each in London, Cardiff, Manchester, Glasgow

6 groups with sophisticated and 2 with less sophisticated users

Consumer Quantitative



2003 face-to-face interviews

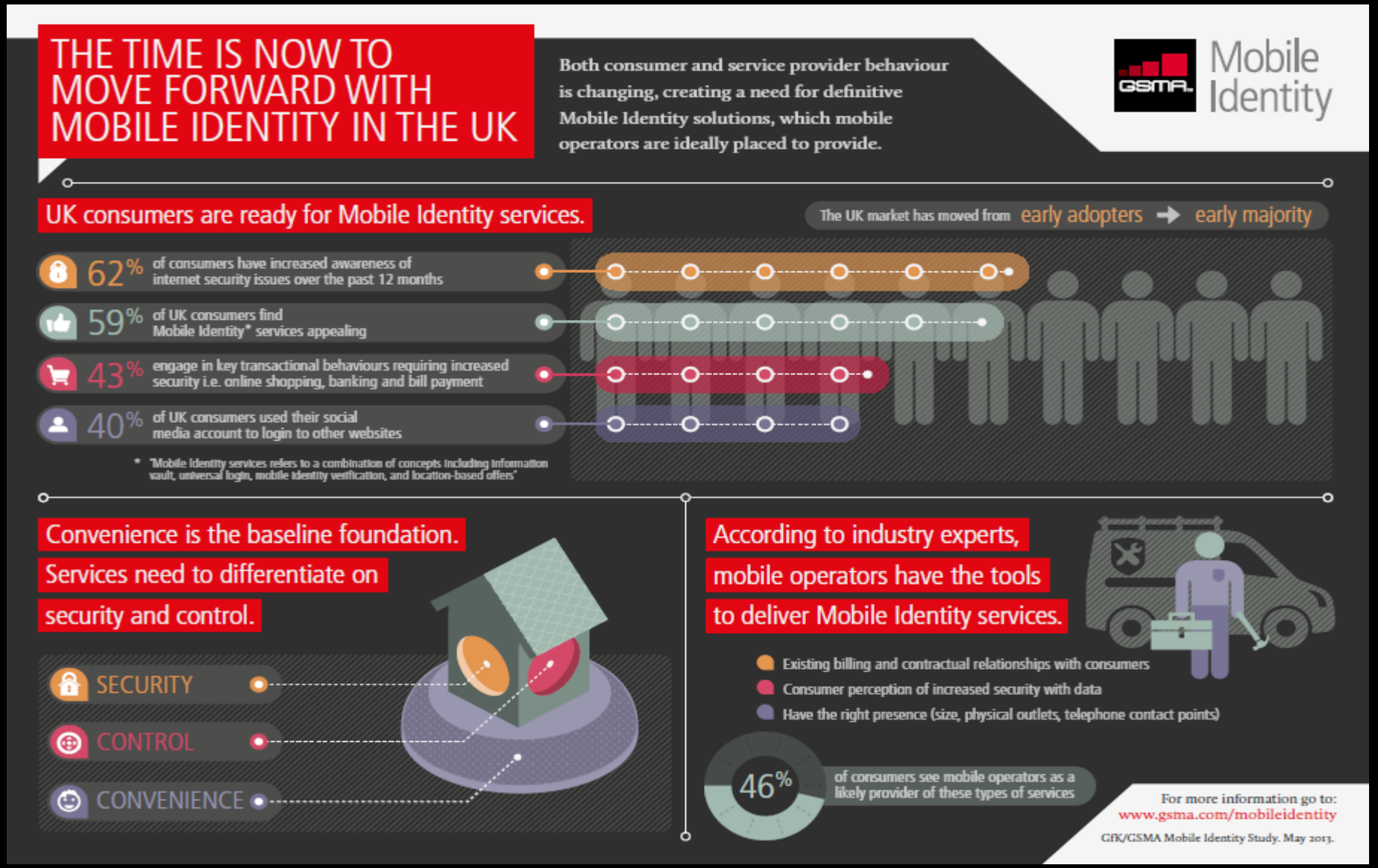
Nationally representative sample of adults aged 16 and over in the UK

Both people with and without internet access were interviewed

Data weighted to age, gender, region, income and internet access

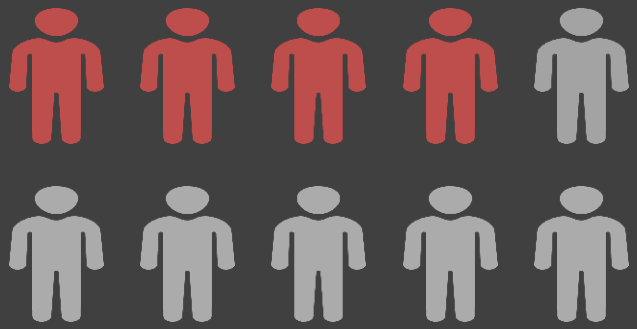
Service providers and consumers in focus groups received incentive of £50 as an incentive for their participation

Summary of key findings



CURRENT CONSUMER CLIMATE

UK consumers are more advanced than expected, driven by convenience, and the market is maturing quickly



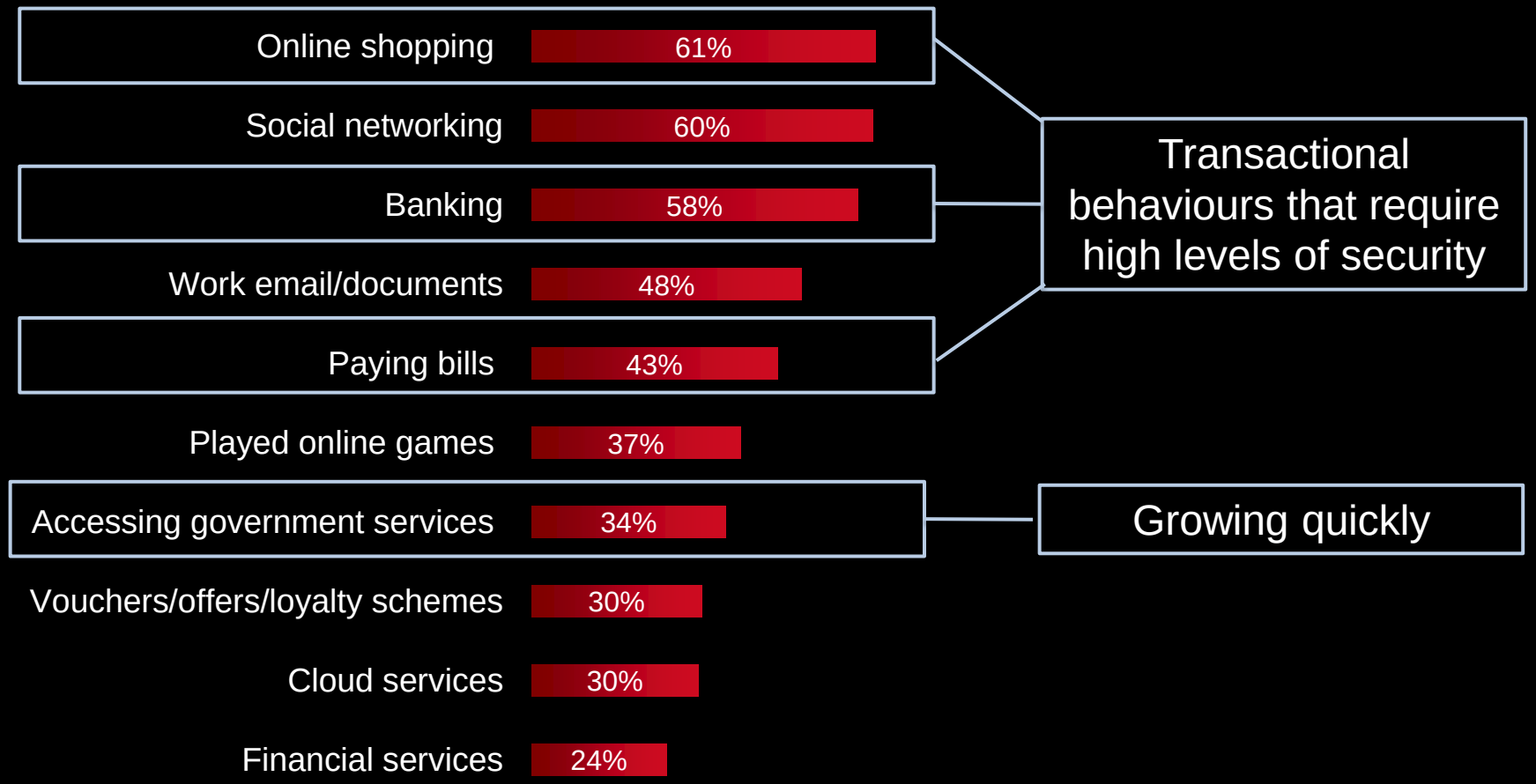
40% of UK consumers have used their social media account to login to other websites



The majority of consumers are becoming more aware of internet security issues – future services will have to deliver more security

Source: Mobile Identity Quant Study
Base: All Respondents (2003)

UK consumers are undertaking transactional behaviours that require higher levels of security



Source: Mobile Identity Quant Study
Base: All Respondents (2003)

However, these behaviours could become almost ubiquitous if poor security was not inhibiting behaviour

Consumer PAIN POINTS with existing security

1. Purchases or sign-up processes have been aborted because user felt insecure with an unknown, less professional looking retailer

2. Too tedious – too much information required, for example needing to set up a profile to read an article

3. Worried about lack of control: follow-up sales calls – when getting insurance quote comparison, did not want to provide their contact details

"I looked at a product I wanted on a website, but I wasn't comfortable with it, it didn't look right, and I was not happy to give my bankcard and address. I can find the product somewhere else…"

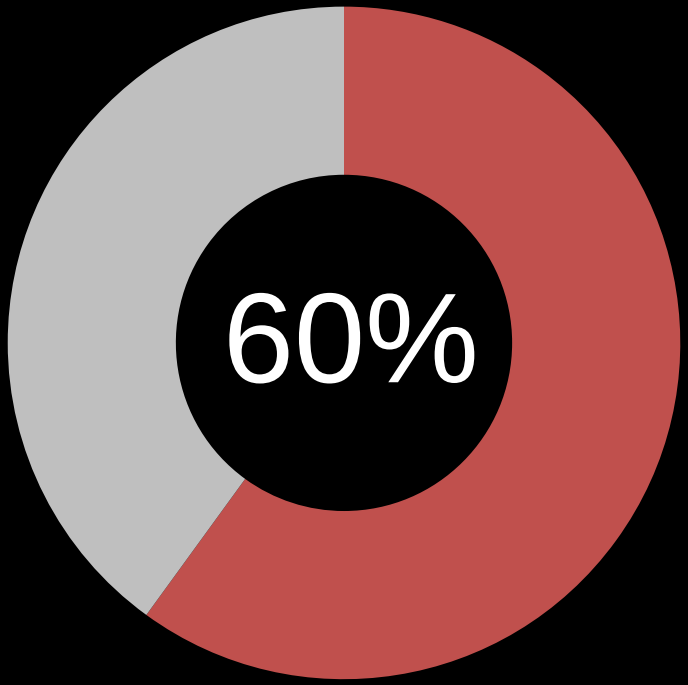
London, sophisticated

"I tend to just stick to the 'safe' ones"

Cardiff, less sophisticated user

Industry experts agree that security is important, but it is still not top of mind for many consumers and they are not adequately protected

Proportion of consumers that change their online passwords once a year or less often



Generally only use trusted and well known sites and brands

So passwords remain unchanged, forgotten, written down or simply not used – on the phone or the PC

More worried about the social implications of hacking/fraud (social embarrassment) than financial loss

Because they 'know' they will be compensated for financial fraud

SERVICE PROVIDER PERSPECTIVES

In a maturing digital economy service providers are increasingly in need of digital identity solutions

Numerous PAIN POINTS for service providers…

Lost, forgotten, stolen and broken IDs	Reluctance to use or share passport details	Lack of industry standards causing many inefficiencies	Mixed authentication and verification methods cause problems: hard copies used alongside digital	Some indicate that these manual processes are costing them tens of thousands of pounds
Collecting, processing and storing hard copies of ID	Current methods can take up to a month to complete verification and authentication	Passing up good employees because processes taking too long	Customers are discouraged and are lost to some service providers by outdated and lengthy processes	Keying data often more than once, copying and duplicating forms, searching records

"The painful part is there's a lot of documents to gather. And to visit a solicitor to verify it - we don't accept printouts they have to be originals. The pain is that clients need the documents too and it's a ten day turnaround. Something can get lost and it is slow and it costs us money."
(Service Provider, Banking)

"We get some visibility of the on and offline data. But not much, can link offline journey to online journey - can do that but we don't get the data, we want it but can't get it. Want a closed loop like John Lewis."
(Service Provider, Retail)

Service providers can see how mobile identity can improve current practices and provide incremental benefits

Improvements	Benefits
…speed and reliability of identity transactions, saving money, saving time, improving service and increasing customer base	…create loyalty cards/schemes more efficiently and effectively
…interactions with government agencies	…enhance CRM capabilities
…the level of internal security and provide a solid audit trial of employees	…improve speed and scope of recruitment process – instant background checks
…usability of provider websites: faster processing and easier purchases increasing business	…cross-referencing marketing initiatives between companies – create a singular retail experience for consumers

Service providers want leadership regarding how digital identity solutions can be shaped and rolled out

Service Providers have high expectations around mobile operator ability to launch and manage the process

- Agreement between providers on a common way forward to ensure the customer numbers add up
- Standards: how and what to host and where to host the data
- A trust framework to ensure customers are re-assured
- To show leadership in innovation
- To ensure Government understand the commercial realities of digital and mobile identity
- To show Government that mobile operators can work together as a self governing and self regulating body

THE CONSUMER PROPOSITION

Appeal for the concepts tested was high, with the combined concept testing above average

52%	54%	56%	49%	59%
				
Information Vault (Attribute Brokerage)	**Universal Login (Federated Identity with Second Factor Authentication)**	**Mobile Identity Verification (e.g. Age)**	**Location-Based Offers**	**Combined Concept**

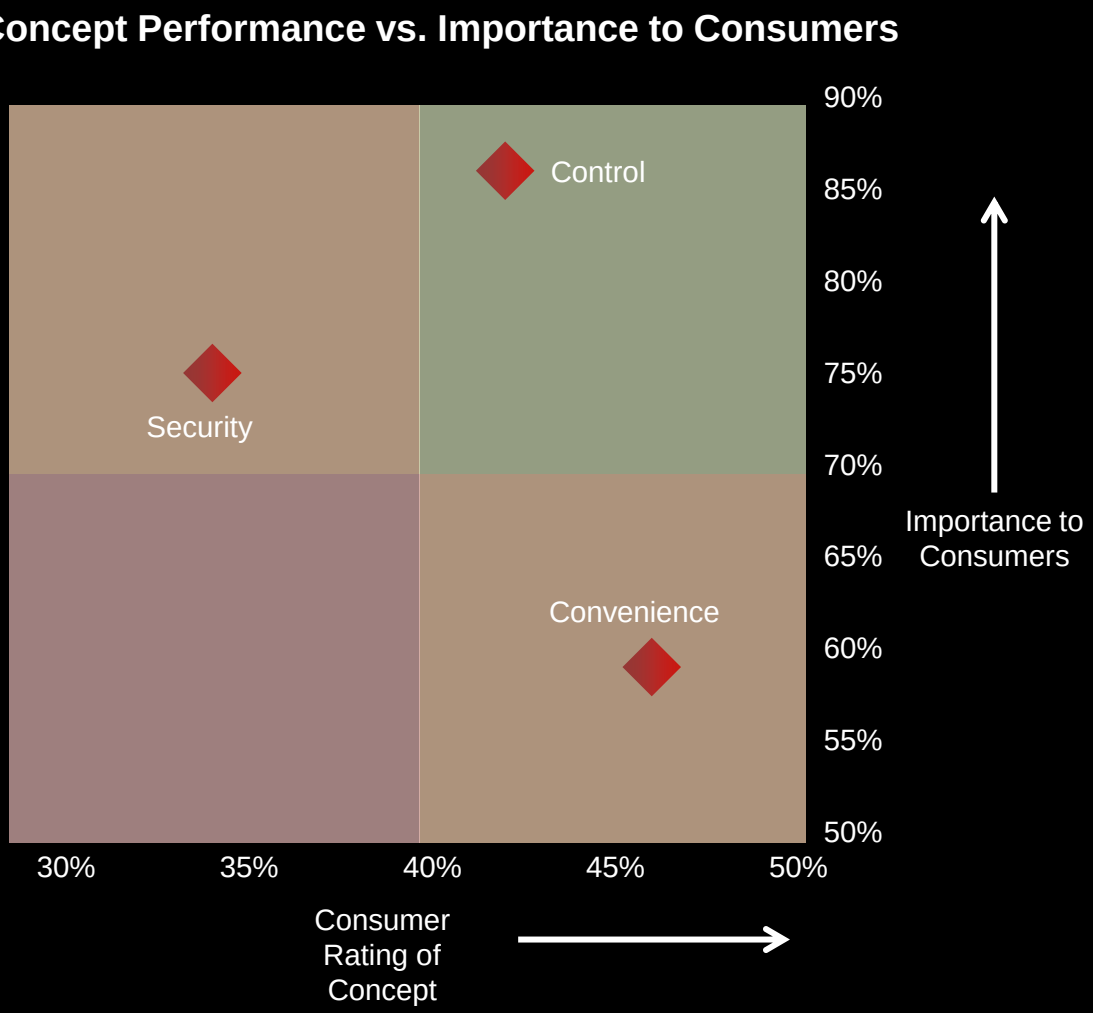
Concept Appeal ranks as Above Average against GfK's concept norms

Source: Concept Appeal – Fairly / Very / Extremely Appealing
Base: All Respondents (2003)

To attract consumers, mobile identity solutions need to match (or better) convenience of existing services and differentiate on security and control

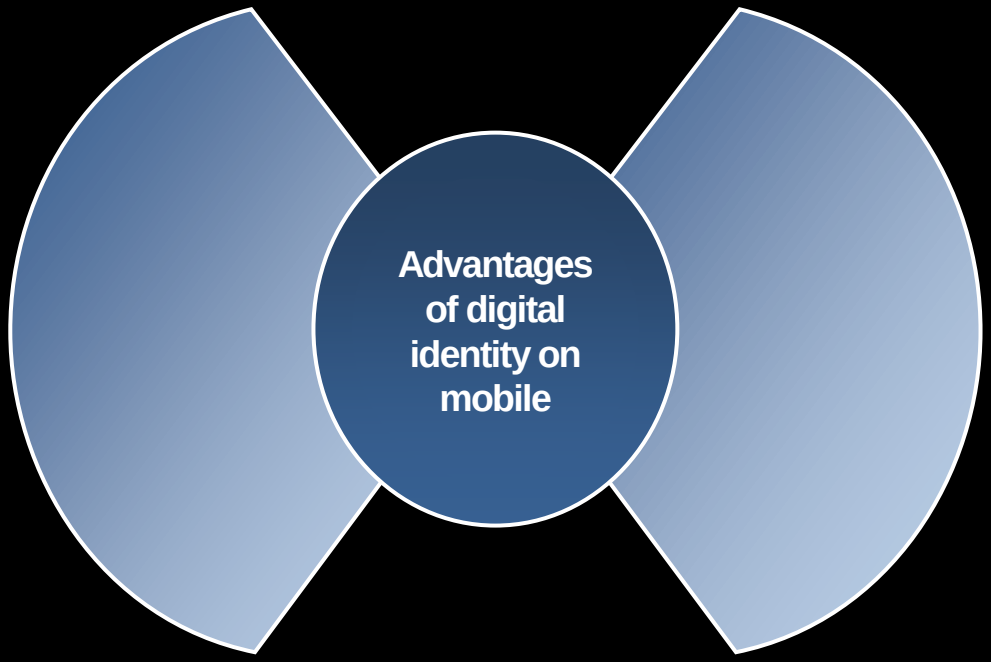
Security and Control have the potential to be USPs and push ahead of other services

Convenience is a necessary hygiene factor



Source: Mobile Identity Quant Study
Base: All Respondents (2003)

Industry experts are quick to identify many advantages of running digital identity over the mobile phone



Secure

Quickly know if it is lost/stolen

Great display

Computing power

Always with user

Simple usability

Convenient

Fun for the user

'"The obvious thing to use is the mobile phone - it has the display, the computing power and it is the most common thing people will carry with them. Mobile is the convenient device. It needs to be mobile because you will want to establish your ID in many, many scenarios."

Communication is required to address consumers' common concern of losing their mobile phone

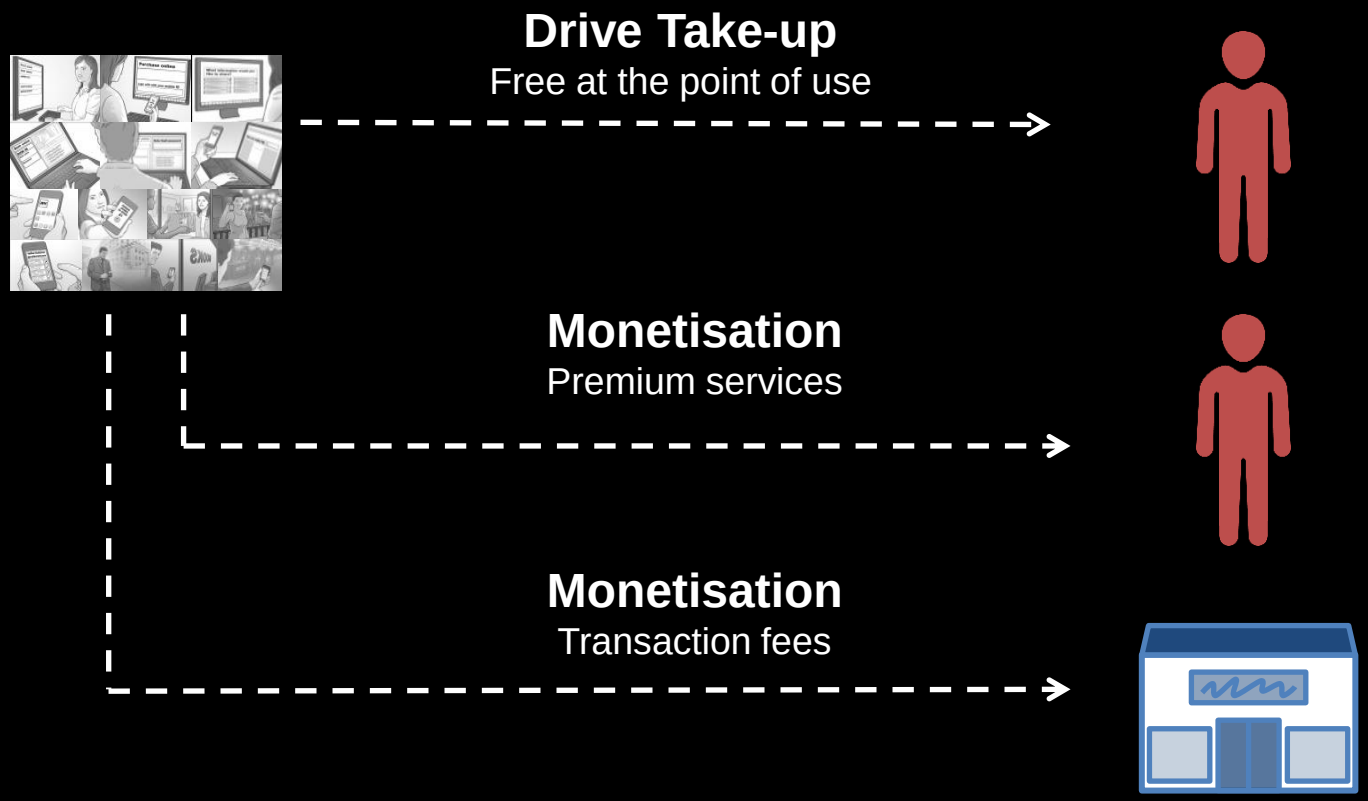
A lost or stolen phone not PIN protected: mobile identity is accessed and abused

Need re-assurance on data security as most feel any solution is vulnerable to hacking

All in one place as opposed to scattered across different services, or offline too big a risk for some

Questions over the data holder/solution and their credentials in this area: would the data be abused?

Monetisation in the UK is likely to be based on a freemium model for consumers and a transaction fee model for service providers



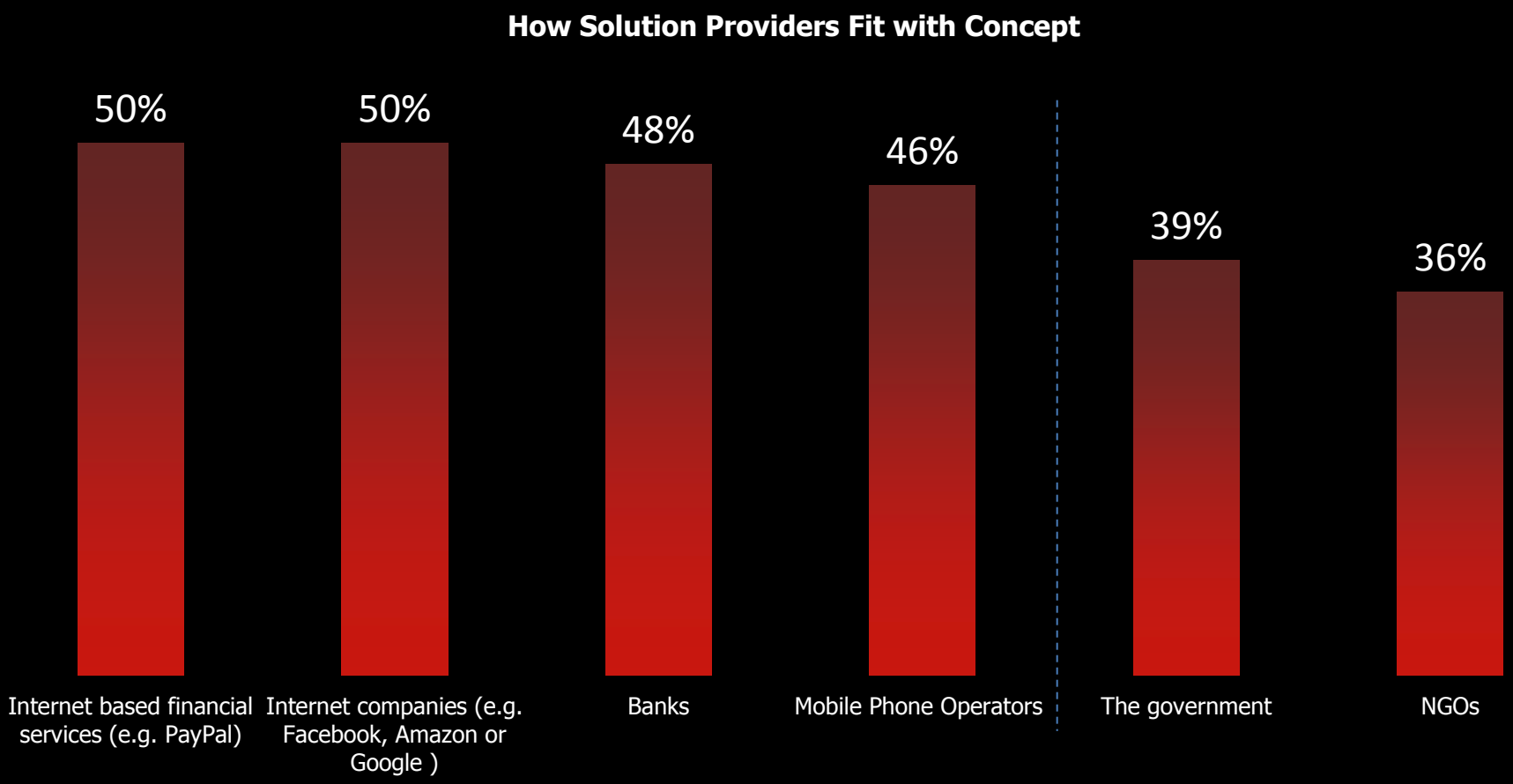
PERCEPTIONS OF POTENTIAL SOLUTION PROVIDERS

Industry experts identify many benefits associated with mobile operators launching digital identity



- Have a billing and contractual relationship with consumers
- More secure with data, in consumers mind
- Have the right ‘presence’ – are large, have face-to-face outlets and have good telephone contact points
- Point to examples of work already happening in this area
- Are independent, can switch provided the right frameworks are in place

Consumers perceive a variety of potential solution providers, with mobile operators ranking in the top four



Source: Mobile Identity Quant Study
Base: All Respondents (2003)

To gain traction with consumers both security and convenience need to be inherent in the service, mobile operators are perceived to deliver both

Consumer perceptions of solution provider strengths

BANKS

Mobile Operators

PayPal

INTERNET COMPANIES





Security ⟷ **Convenience**

Scale of consumer needs

CONCLUSION

The time is now for mobile identity



Service Providers have a need for it

"It's growing faster than we anticipated. It converts so quickly, we are not keeping up but optimising it is an issue"

Consumers are ready for it

Increased use of social media for login + increased awareness of security issues + increased transactional behaviours requiring more security + concept appeal