

LexisNexis® Risk Solutions Millennial Study Privacy vs. Customer Experience



The millennial customer: privacy vs. customer experience.



How much friction will Millennial customers tolerate in transacting with communications companies, banks, payment providers, and retailers?



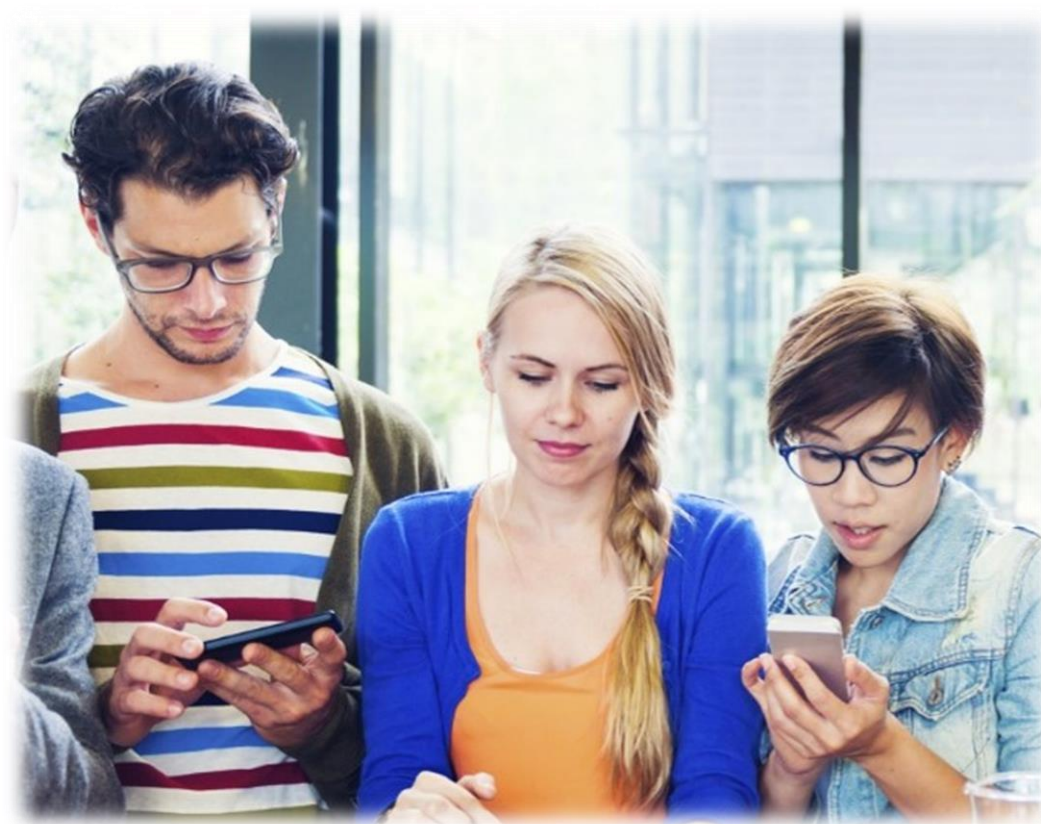
The findings offer valuable insight into millennials' attitudes on information sharing and authentication preferences to enable you to customize identity proofing processes for a better customer experience.



LexisNexis retained KS&R, a global market research firm, to conduct a research study on millennials' behaviors and attitudes on information sharing and authentication preferences.

The methodology of this study comprised:

- Comprehensive survey of 2,804 Millennials, deployed during April-May 2016 across 7 markets: US, UK, Germany, Mexico, Brazil, Hong Kong and Malaysia.
- Respondents represented both younger (18-24 years old) and older (25-34 years old) Millennials.
- The overall margin of sampling error is +/- 1.85% at the 95% confidence level.
- Data reflects the population based on weighting to individual country Census.



Who are Millennials?

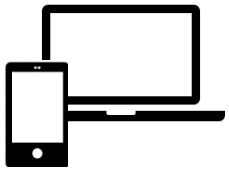


Per Country Profile of Millennials

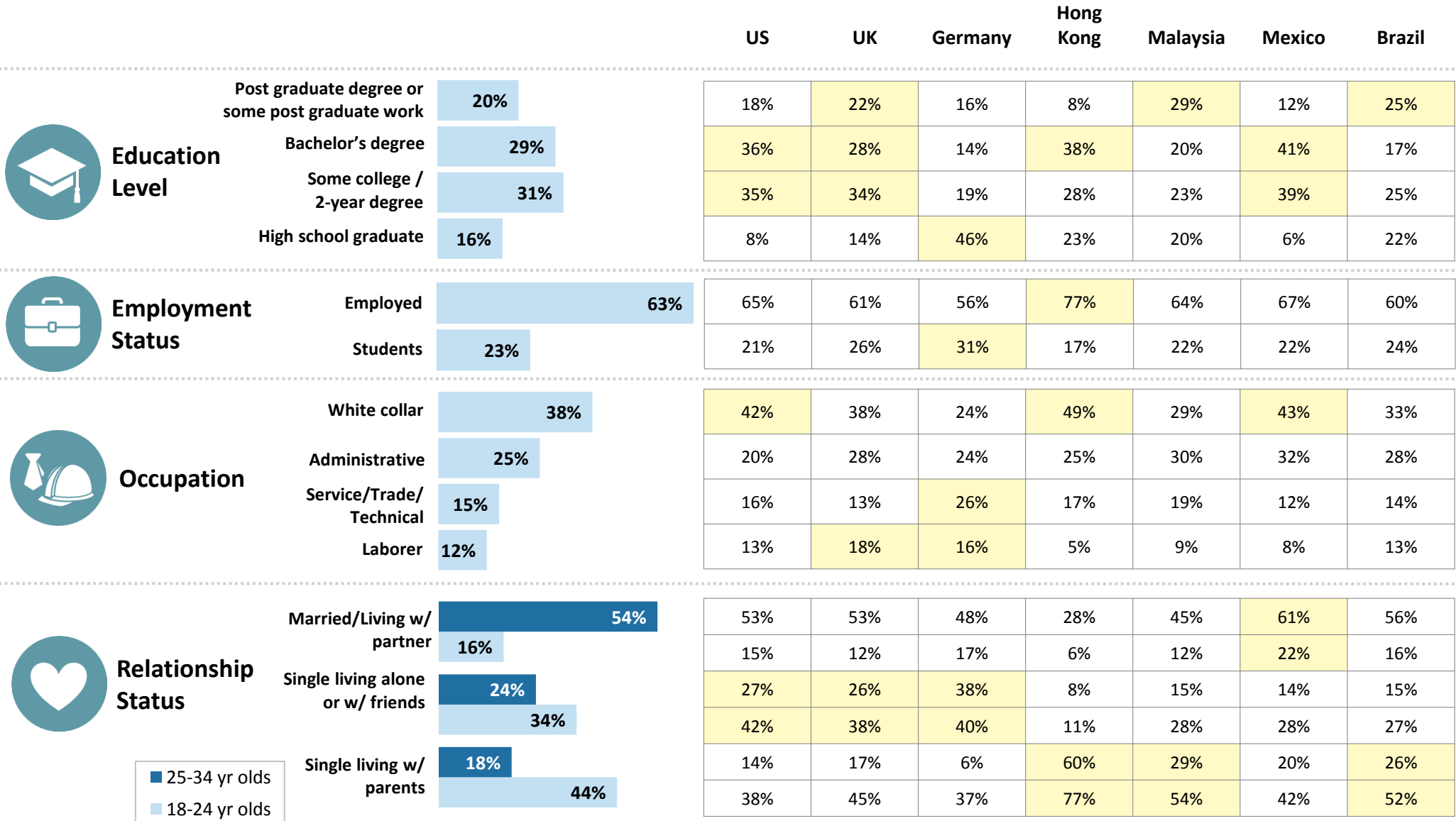
Use of Financial Services



87% use traditional banks



Only 25% use online-only investment banks (e.g., E*trade, ING, Ally Bank)



■ 25-34 yr olds
■ 18-24 yr olds

= higher than other countries

Inside the Millennial mind



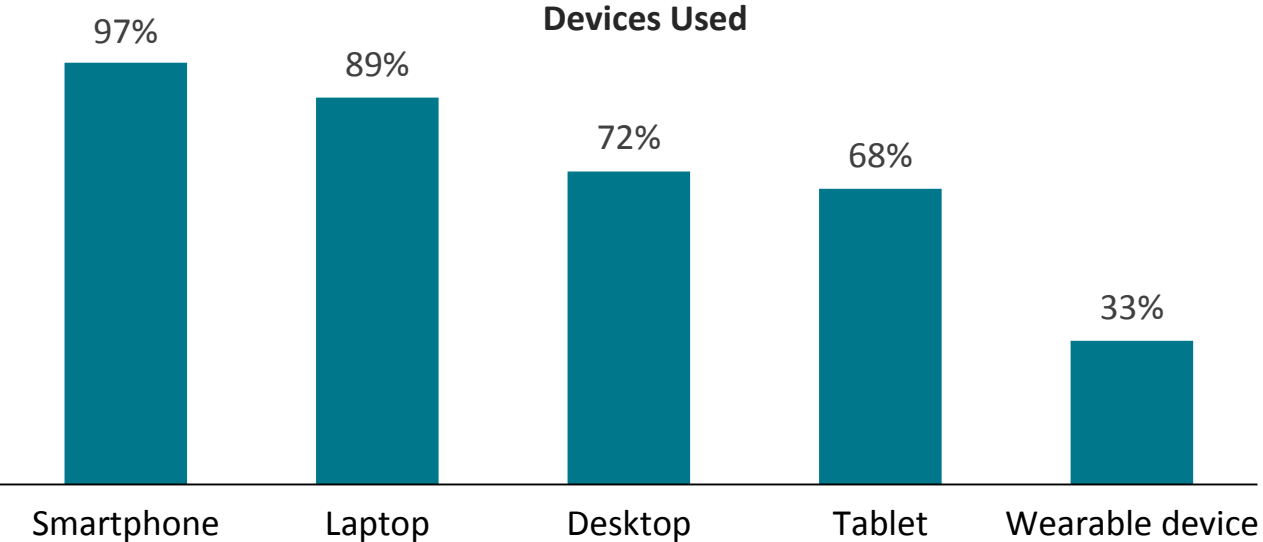
Smartphones and laptops are ubiquitous among Millennials across markets. Tablet use varies, while wearables is still emerging in most countries.

On average, they use 3 – 4 different types of devices.

Those in the UK and Mexico are more likely than others to use laptops, while those in Hong Kong have higher desktop usage.

Tablets are prevalent in most countries.

Wearables use is still emerging, though is highest in Mexico and Brazil.

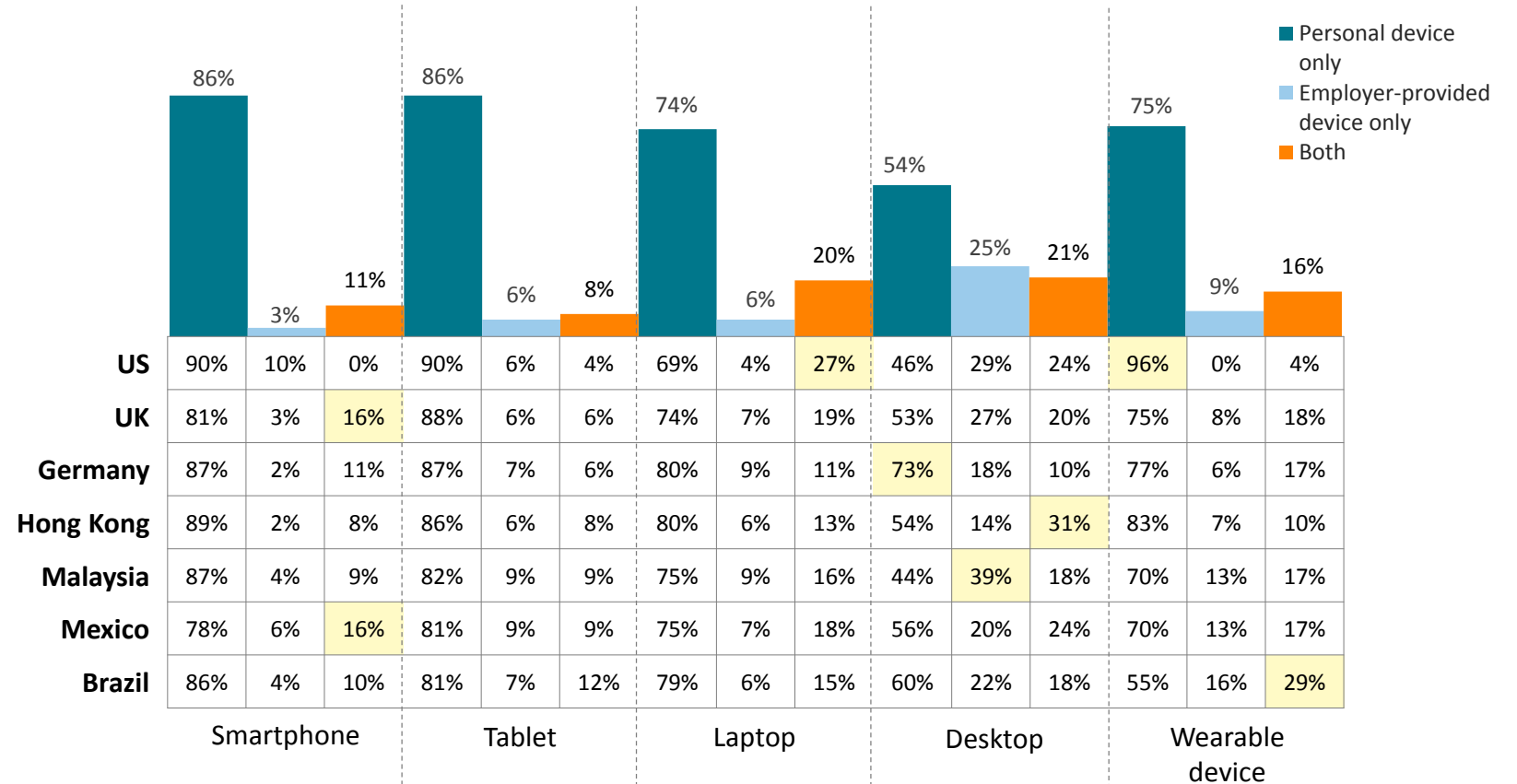


	Smartphone	Laptop	Desktop	Tablet	Wearable device
US	97%	89%	65%	71%	31%
UK	96%	93%	55%	60%	19%
Germany	98%	81%	78%	72%	21%
Hong Kong	98%	82%	92%	74%	33%
Malaysia	99%	86%	67%	56%	32%
Mexico	98%	93%	83%	77%	44%
Brazil	95%	89%	80%	59%	39%

Most devices, across countries, are personal (not provided by an employer).

Where there is a higher likelihood to have both personal and employer-provided devices, this is more often for desktops within many countries.

Personal vs. Employer-Provided* Devices
(among users of each device)

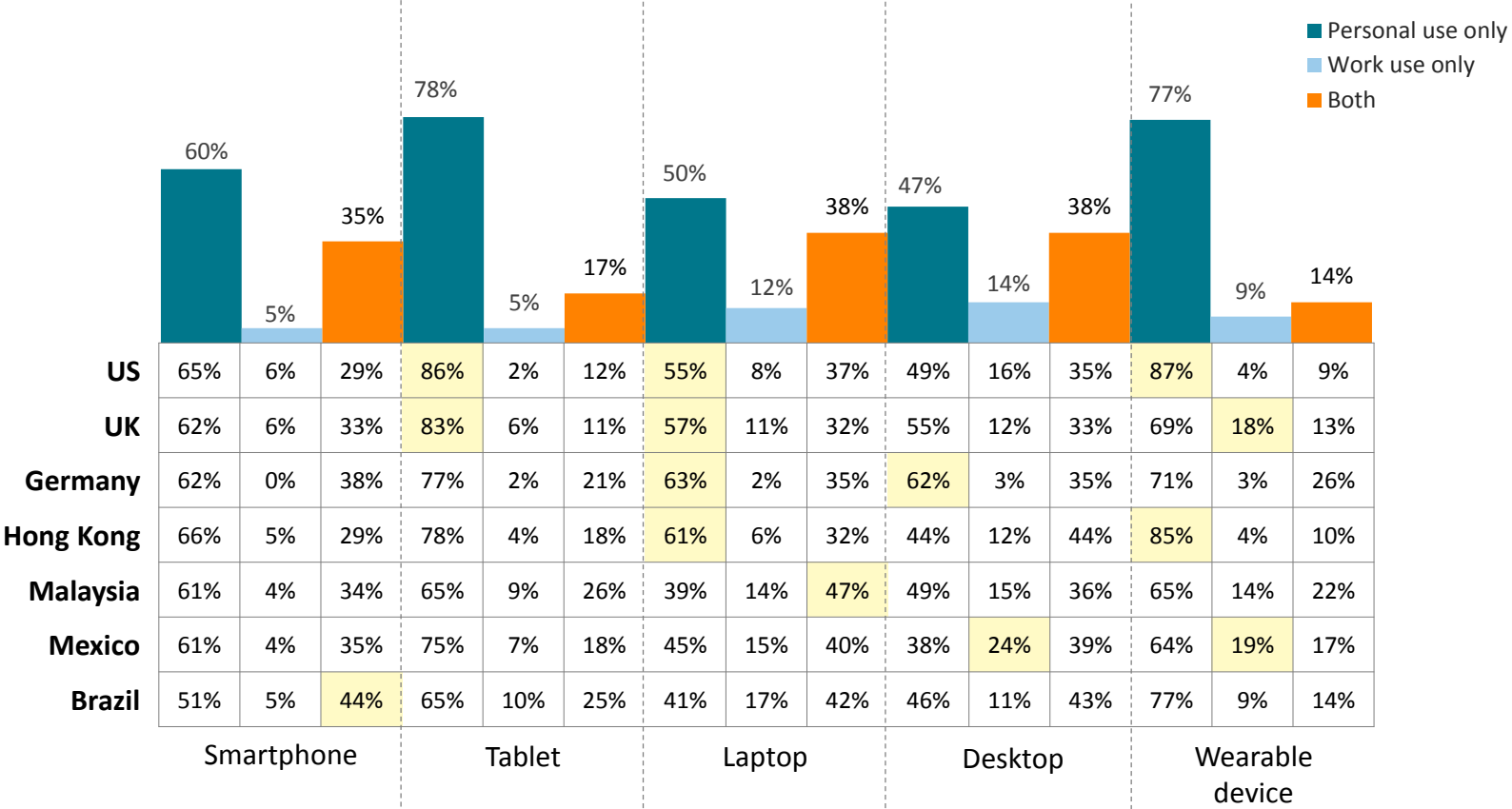


However, a number are using these personal devices for both business and personal activities.

Among smartphone users, Brazilian Millennials are more likely than others to use this device for both personal and business.

Tablets are used more for personal activities in the US and UK.

Personal vs. Work* Use
(among users of each device)



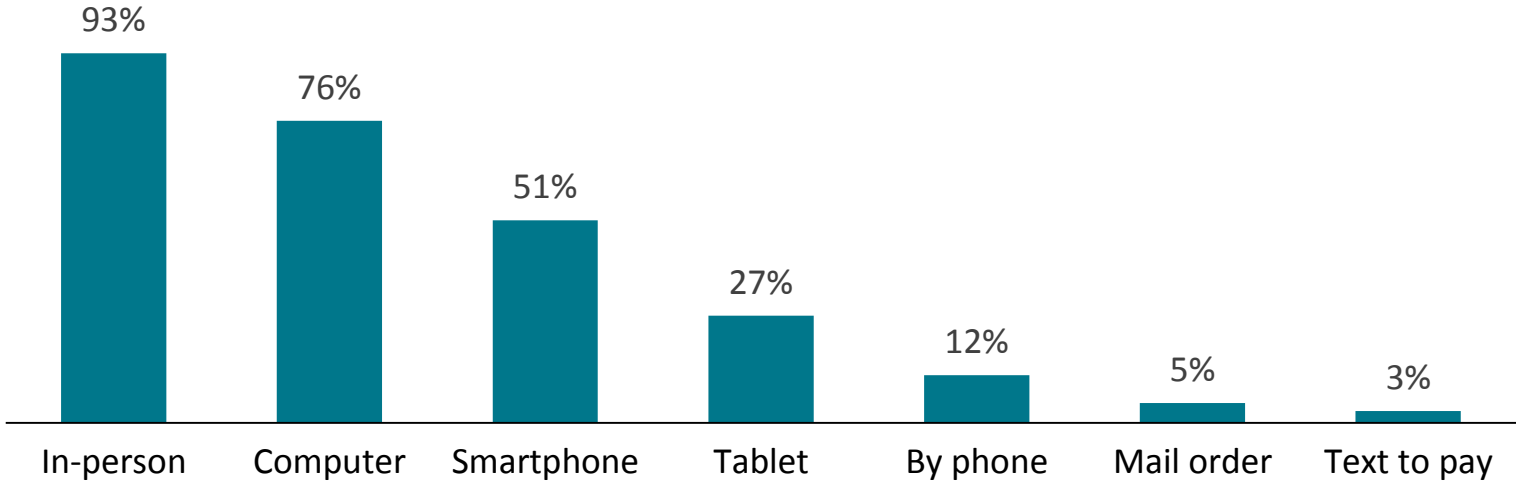
When Millennials shop, they do so in-person and remotely. The computer is the primary remote shopping device, particularly in the UK, Hong Kong, and US.

Smartphone shopping is more prevalent among US Millennials.

M-commerce via a tablet is limited among Millennials across markets.

Shopping by phone is less common overall, but more likely among Hong Kong Millennials than others.

How Millennials Shop

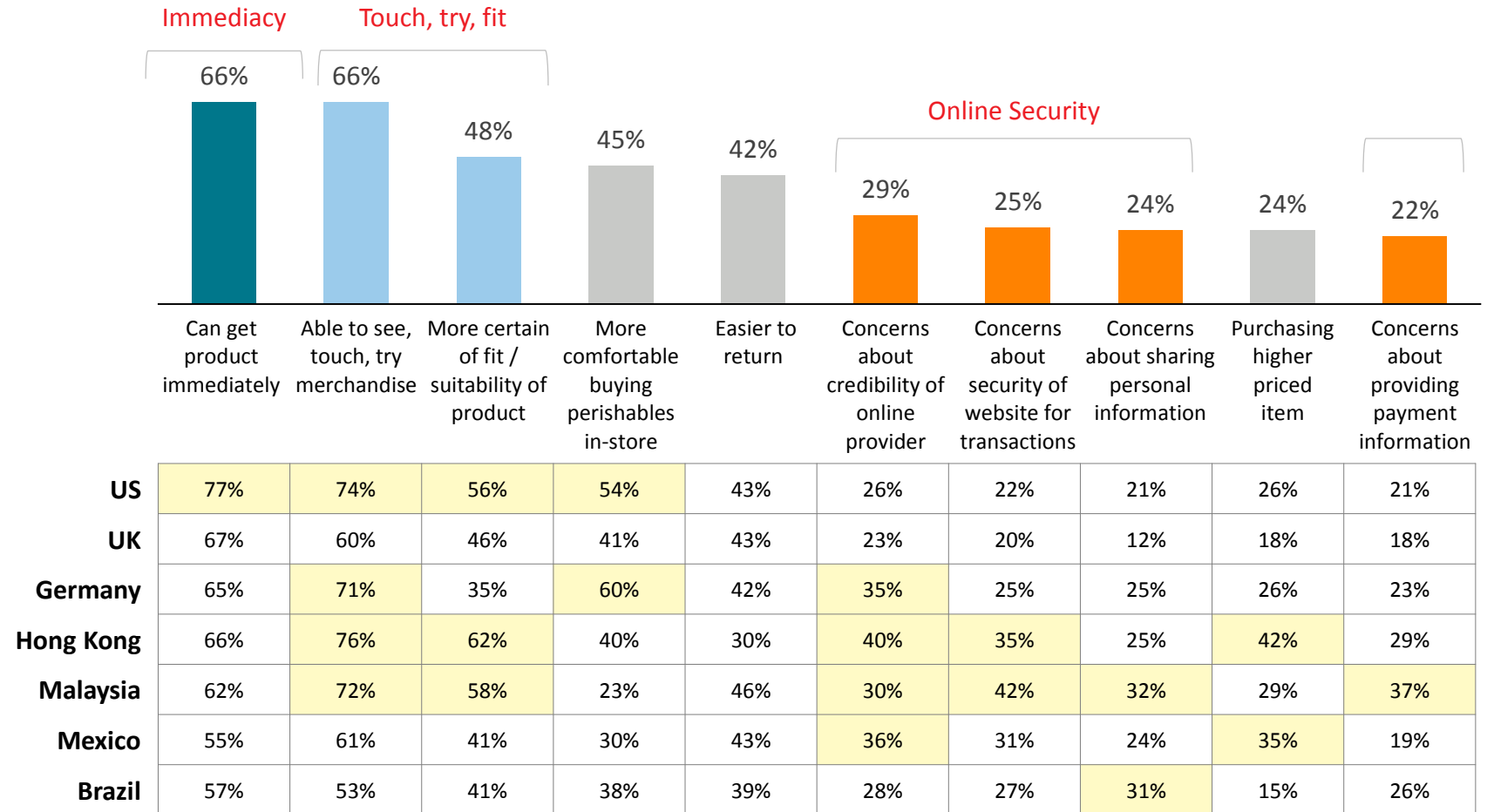


	In-person	Computer	Smartphone	Tablet	By phone	Mail order	Text to pay
US	95%	82%	65%	34%	11%	2%	2%
UK	93%	89%	47%	29%	14%	3%	2%
Germany	95%	63%	54%	30%	9%	16%	5%
Hong Kong	97%	85%	57%	39%	30%	12%	4%
Malaysia	87%	67%	48%	27%	17%	8%	7%
Mexico	97%	68%	38%	22%	19%	5%	6%
Brazil	89%	71%	38%	16%	11%	7%	3%

In-person shopping is driven more by immediacy and ability to see merchandise than by concerns about online security, particularly in the US.

Millennials in Germany, Hong Kong, and Malaysia are also eager to see merchandise in person, but also have more concerns with provider credibility, website security, and/or sharing of information than others.

Reasons to Shop In-Store Rather Than Online



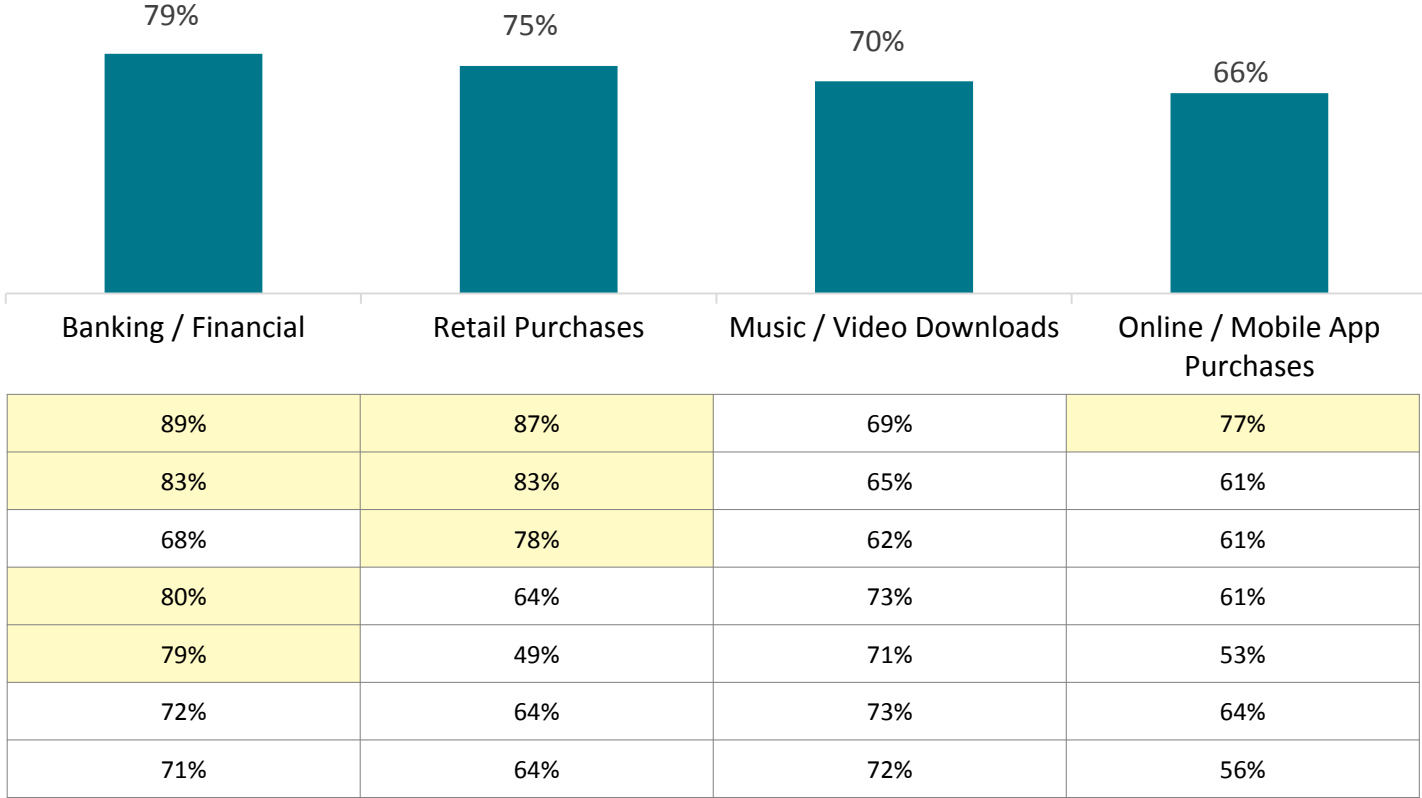
US and UK Millennials are most active with remote activities, including being more engaged with both financial and retail transactions than others.

That said, other Millennials are actively conducting such transactions, but not among quite as many as in the US and UK.

Remote banking is most common among US, UK, Hong Kong, and Malaysian Millennials.

US Millennials are also heavy online / mobile app purchasers.

Transaction Types Conducted Remotely
(among users of each device)



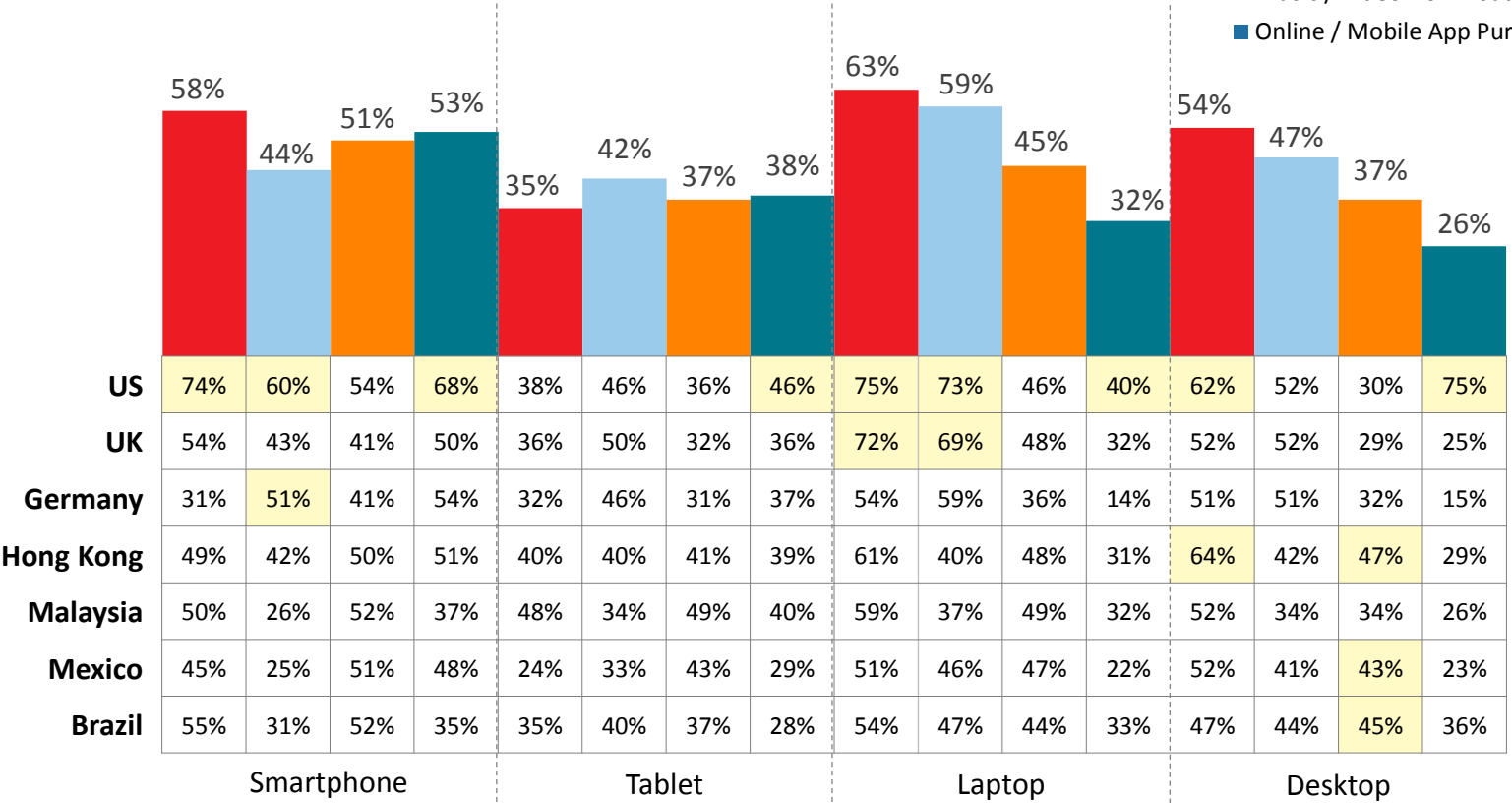
US Millennials are more likely than others to conduct banking, retail purchases, and app purchases on most devices.

Across most markets, tablets are used less often for banking and / or retail purchasing.

Outside of the US, there are few significant differences in Millennial behavior towards using certain devices for certain transactions. Where this differs, German Millennials appear more with regards to using a mobile device (smartphone, tablet) for financial transactions.

Transaction Types Conducted by Device
(among users of each device)

- Banking / Financial
- Retail Purchases
- Music / Video Downloads
- Online / Mobile App Purchases

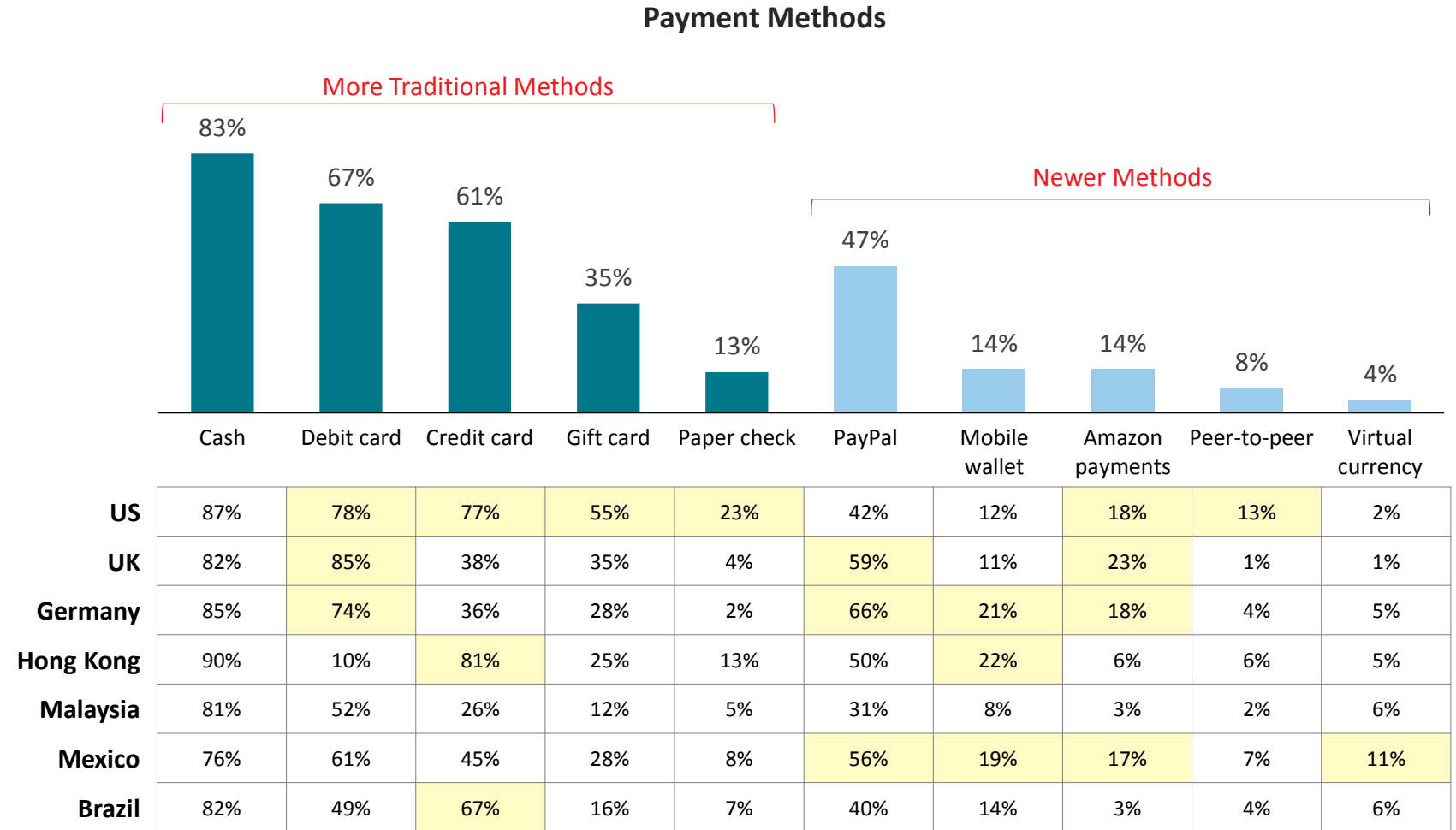


Millennial payment methods differ by region.

Debit card use is more prevalent in the US and Europe

PayPal is more prevalent among European and Mexican Millennials, while other 3rd party methods are still emerging across markets.

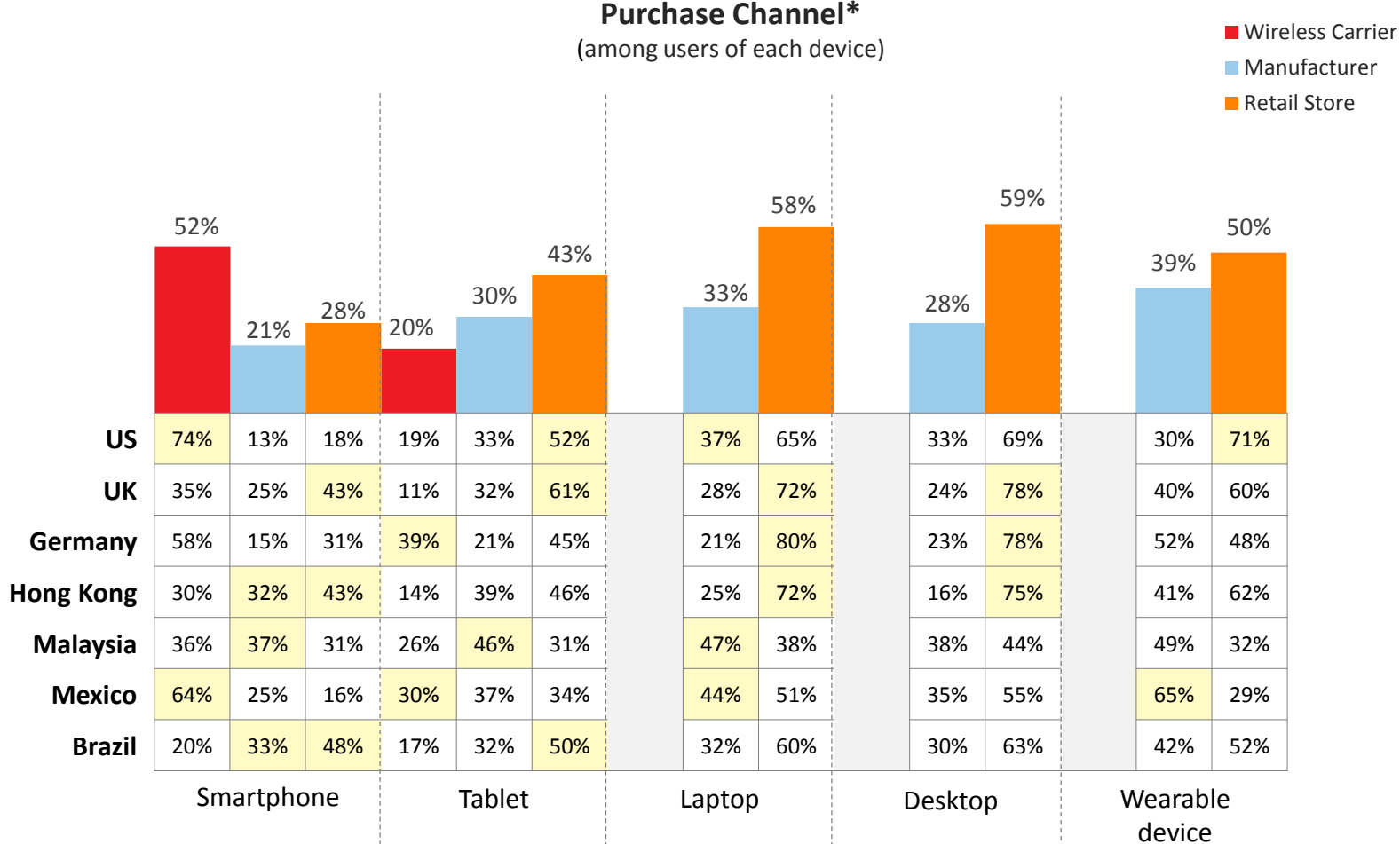
Malaysian Millennials are a bit of a wild card with payment methods. There is no sizable majority for non-cash methods tested, which suggests that they are varied in terms of remote payment methods or are using further methods not tested or explicitly listed in the survey.



Channel use varies by region / country for Millennials' purchases of different devices.

As the North American model, US and Mexican Millennials are more likely than others to purchase smartphones through the wireless carrier. The Retail channel is more prevalent for smartphones in the UK, Hong Kong and Brazil.

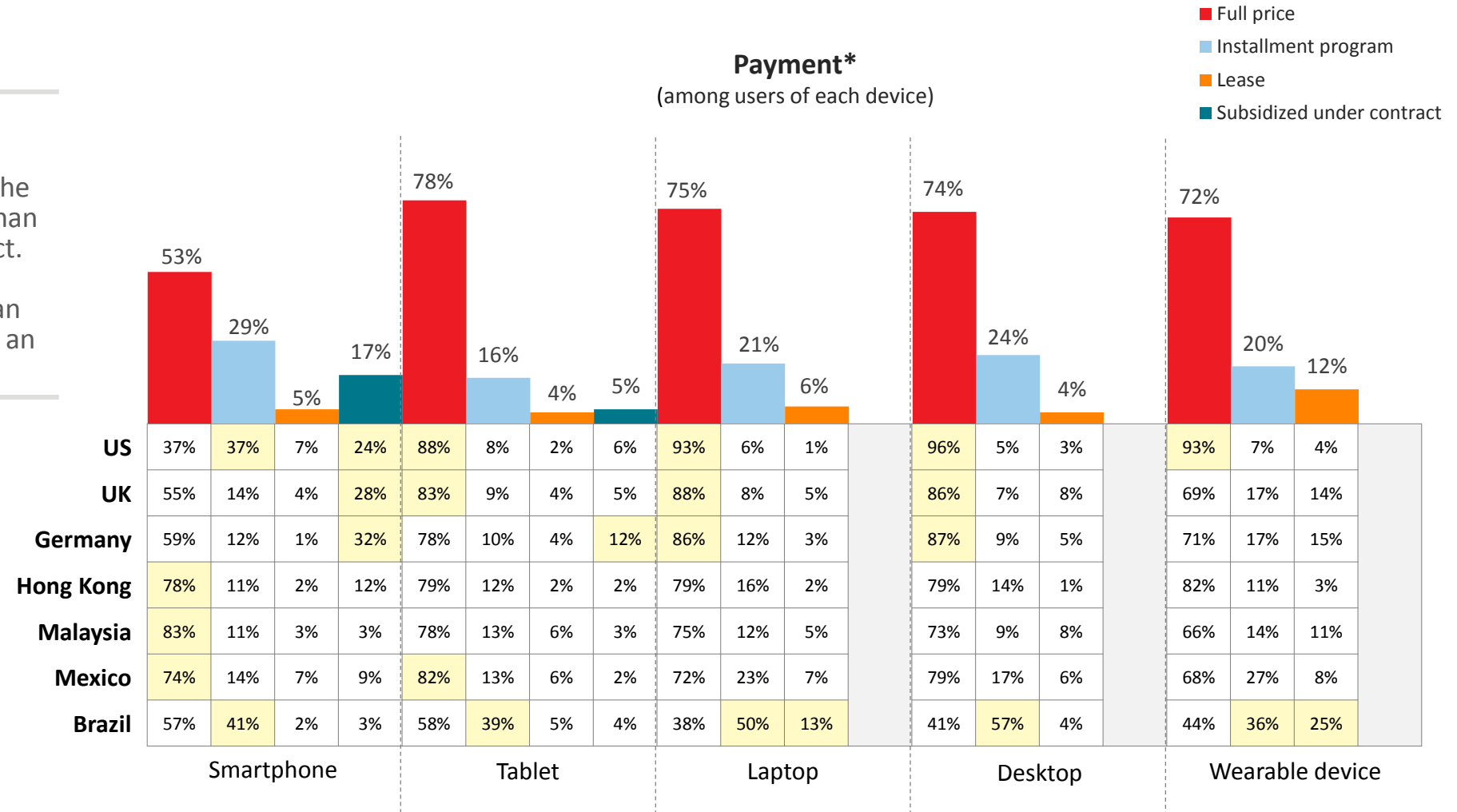
For other devices, channels tend to vary by region. Retailers are Millennials' choices (options) for computers in the US, Europe and Hong Kong, while channels are mixed for these devices in other markets.



US, UK, and German Millennials are more likely than others to pay full price for tablets, laptops, and/or desktops.

Hong Kong, Malaysian, and Mexican Millennials are more likely to pay full price for smartphones, while those in the US, UK, and Germany are more likely than others to subsidize them under contract.

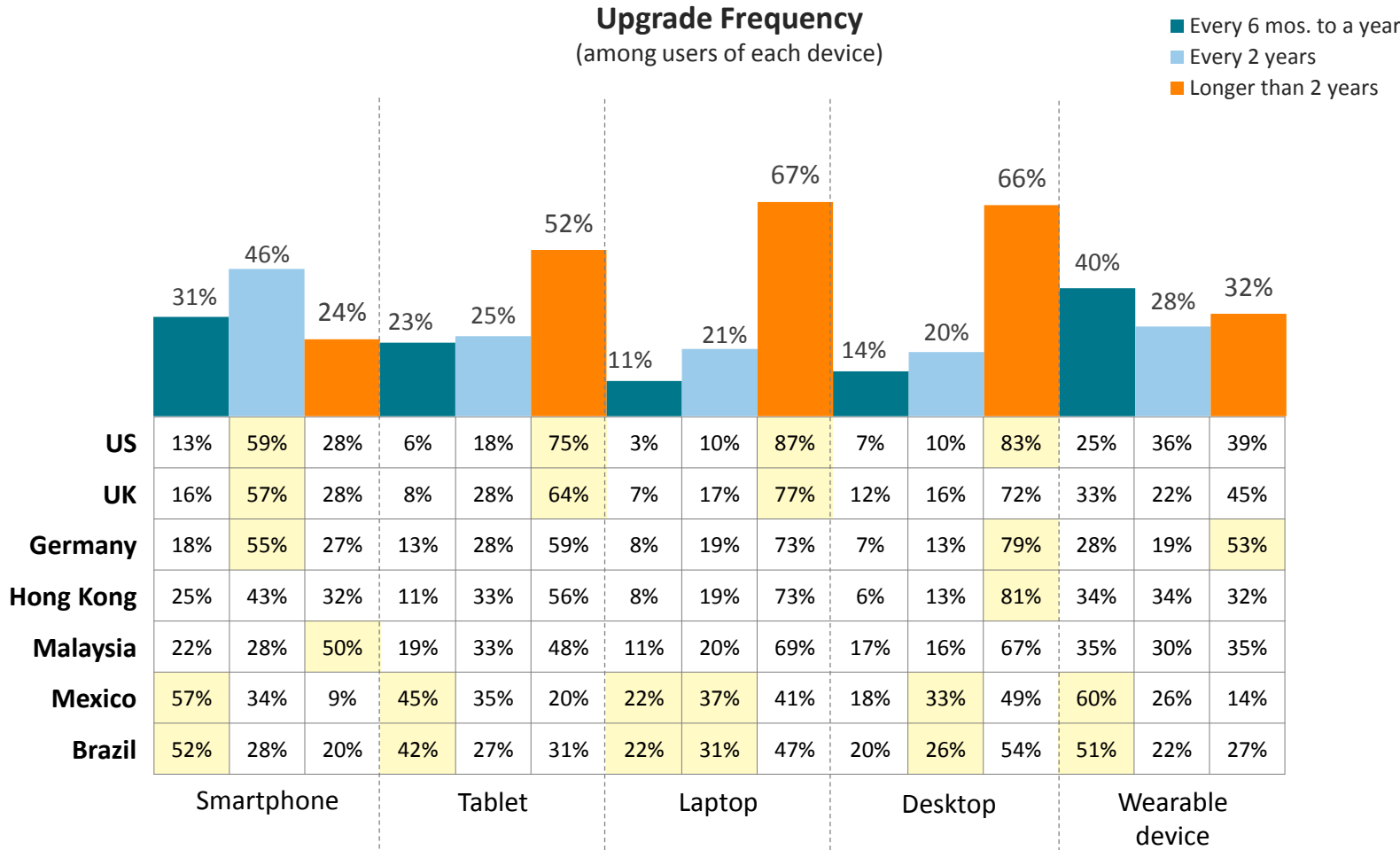
Brazilian Millennials are more likely than others to purchase their devices under an installment program.



Except for Malaysia, Millennials across markets are more likely to swap their smartphones sooner than other devices.

Brazilian and Mexican Millennials are more likely to swap / upgrade their devices sooner than Millennials in other markets.

US and UK Millennials wait longer than others to upgrade their tablets and laptops.

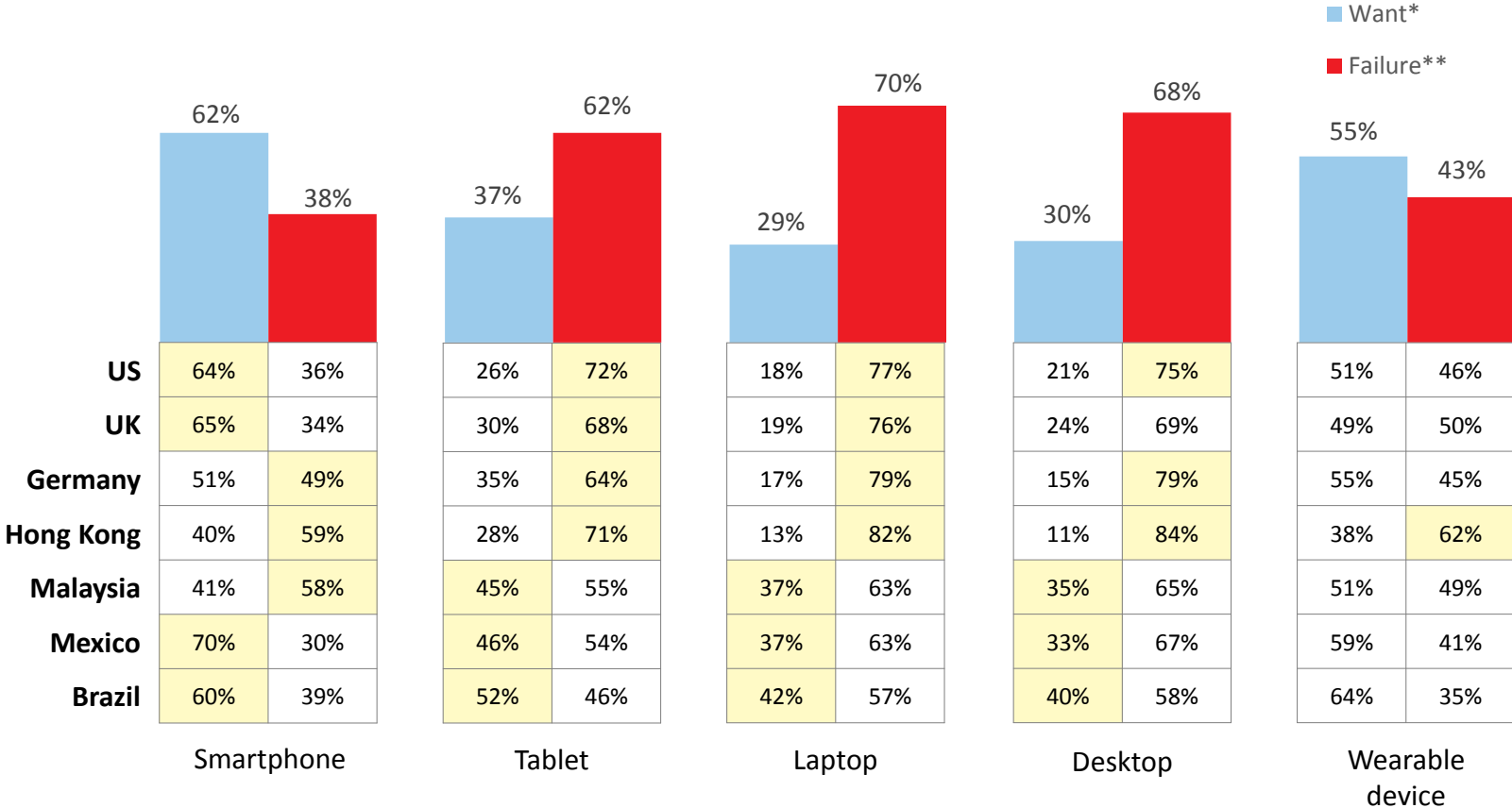


Brazilian and Mexican Millennials are more likely than others to upgrade their tablets , laptops, and desktops out of want (rather than need) .

US and UK Millennials join them in wanting the latest smartphone.

US, UK, German, and Hong Kong Millennials tend to wait until their other devices fail before replacing.

Reasons for Upgrade
(among users of each device)



Q: What is your primary reason for replacing your device?
 *Those who selected "Want latest model" or "Mobile contract allows"
 **Those who selected "Device stopped working" or "Device became obsolete"

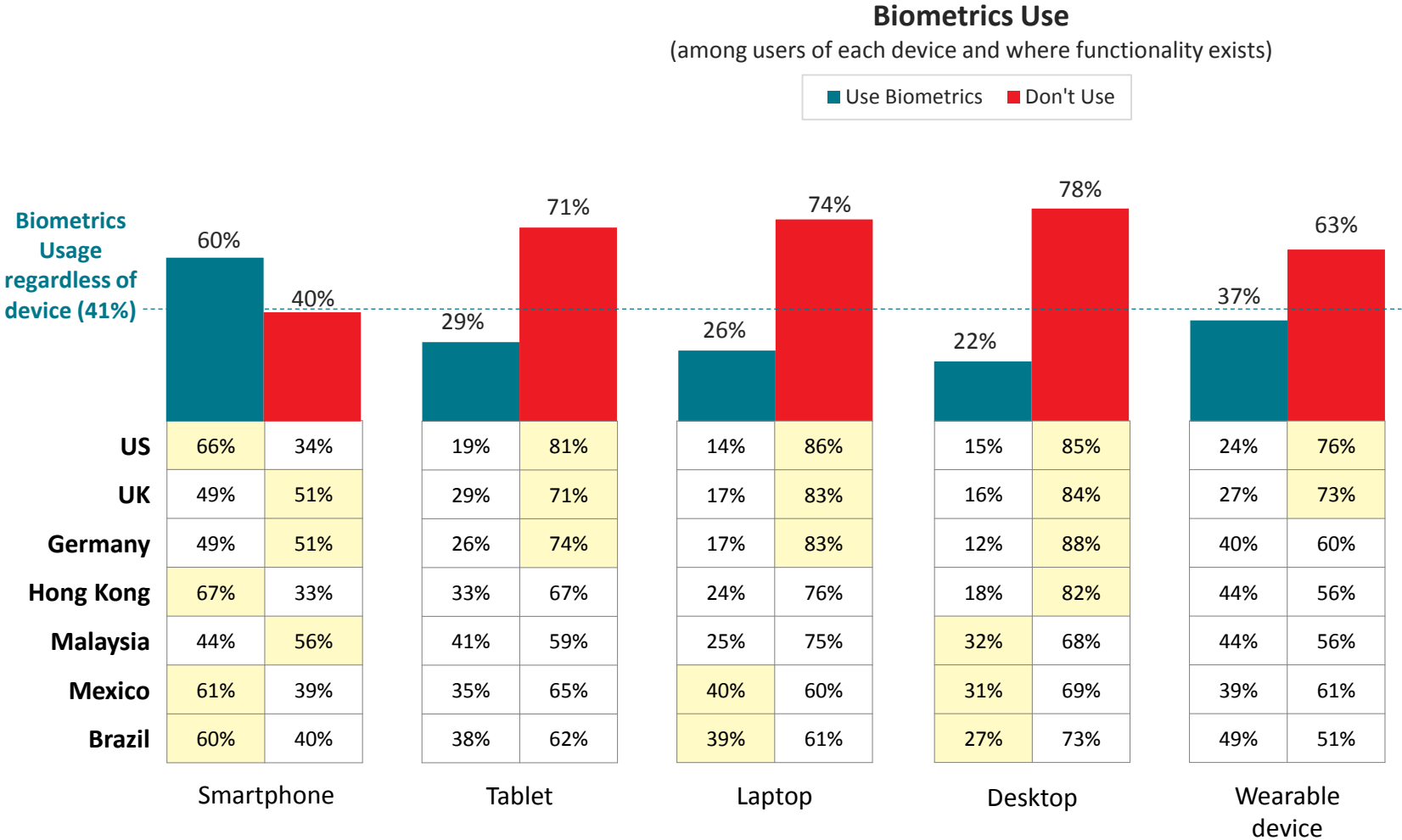
 = higher than other countries

Is trust an issue?



Biometrics use is fairly strong with smartphones, particularly among US, Hong Kong, Mexican, and Brazilian Millennials.

US, UK, and German Millennials are less likely than others to use Biometrics on other devices.



Malaysian, Mexican, and Brazilian Millennials are most worried about having their identity and debit/credit card info stolen.

But they are also more likely to recognize that companies need their personal information in order to protect them from fraud.

At the same time, they are just as likely as others to be bothered by companies asking for this information and how it is being handled.

	% Rating Agree	US	UK	Germany	Hong Kong	Malaysia	Mexico	Brazil
I worry about having my identity stolen in a data breach	69%	66%	55%	62%	70%	77%	77%	76%
When companies ask me for personal information, I sometimes think twice before providing it	69%	72%	65%	64%	62%	70%	63%	72%
I worry about having my debit card information stolen	69%	66%	58%	55%	57%	77%	78%	77%
I worry about having my credit card information stolen	67%	64%	46%	46%	70%	78%	77%	77%
I believe the risk to my online privacy will increase as society becomes more digitally connected	65%	72%	64%	65%	70%	70%	61%	57%
I worry about having my identity stolen through online / app / mobile activities	65%	62%	52%	52%	67%	78%	74%	73%
I'm concerned that companies are collecting too much personal information about me	63%	58%	58%	63%	66%	72%	60%	73%
I am concerned about the way companies handle my personal information	63%	58%	58%	56%	52%	65%	63%	75%
It is necessary for companies to ask for personal information in order to verify identity and prevent theft / fraud	61%	59%	54%	47%	44%	70%	67%	67%
It usually bothers me when companies ask me for personal information	55%	61%	47%	54%	43%	64%	45%	53%
I am required to remember too many passwords	54%	54%	54%	44%	60%	57%	47%	61%
I would be willing to provide a summary of my shopping habits in exchange for "free" products or services	54%	61%	47%	45%	41%	48%	49%	51%
I worry about having my identity stolen in person	54%	44%	37%	36%	66%	69%	69%	71%
I feel more comfortable when companies ask for personal information in order to verify identity	43%	42%	35%	31%	46%	55%	50%	48%
I would be willing to provide access to my geographic location in exchange for targeted goods or services	36%	34%	32%	32%	47%	41%	37%	42%
I believe my online privacy is completely protected by effective safeguards	29%	23%	26%	17%	48%	49%	40%	33%

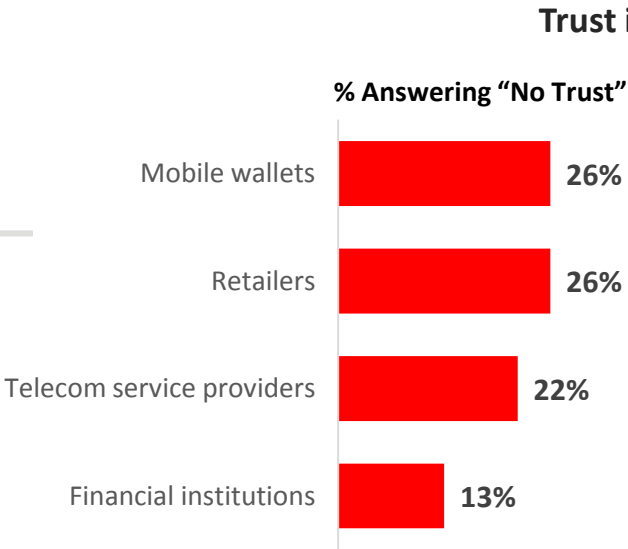
Q: For each of the following statements, please indicate your level of agreement.

= higher than other countries

Distrust with retailers, communications companies and payment providers is sizeable, varying by country.

Retailers are most distrusted among Hong Kong, Malaysian, and Mexican Millennials.

Communications providers are somewhat more distrusted among European Millennials.



Trust in Handling Personal Information

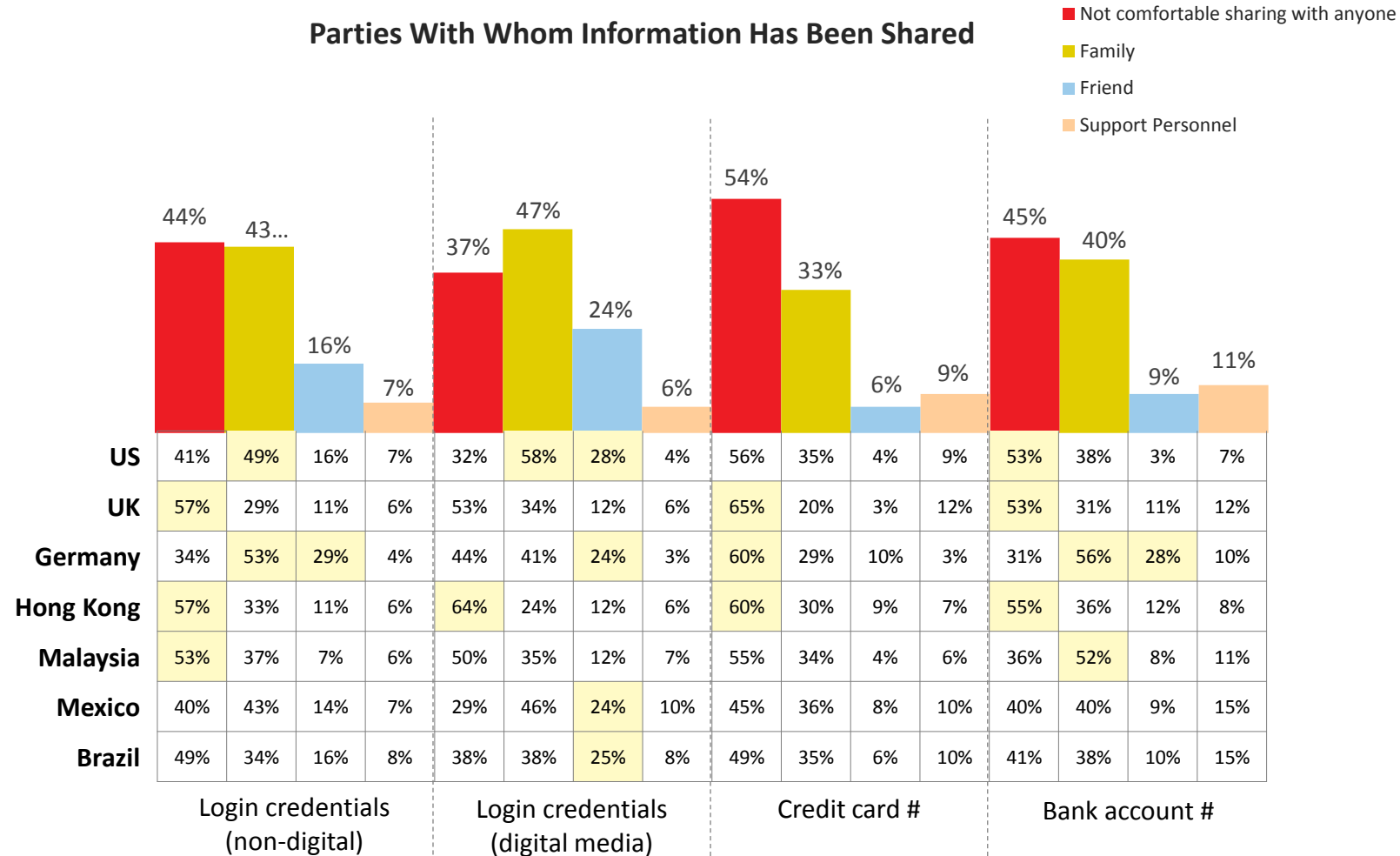
	US	UK	Germany	Hong Kong	Malaysia	Mexico	Brazil
Mobile wallets	31%	24%	25%	17%	33%	16%	25%
Retailers	28%	23%	17%	31%	37%	33%	21%
Telecom service providers	19%	27%	30%	19%	20%	18%	23%
Financial institutions	9%	12%	18%	9%	14%	14%	18%

The types of information shared and with whom vary across countries.

UK and Hong Kong Millennials are less likely than others to be comfortable sharing their information with anyone.

German Millennials are more likely than most others to be comfortable sharing information outside of their bank account number with family and/or friends.

US, Mexican, and Brazilian Millennials are likely to only share non-financial information with family and/or friends.

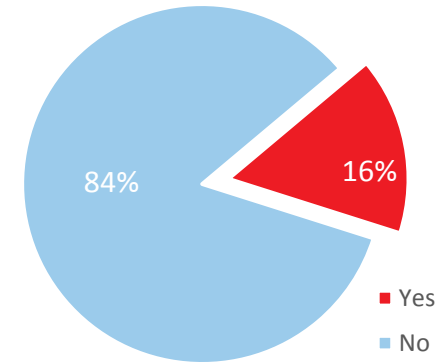


Though only a minority of Millennials have been victims of identity theft, it is more common in the US.

Even so, US Millennials who have been victims of identity theft are likely to be less worried about the long-term impact than others.

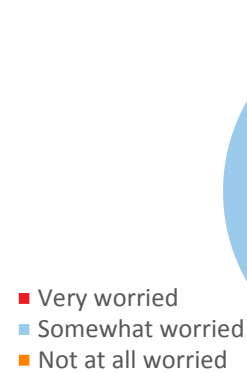
Malaysian and Brazilian victims are most worried about its impact.

Victim of Identity Theft



	No	Yes
US	80%	20%
UK	91%	9%
Germany	90%	10%
Hong Kong	86%	14%
Malaysia	83%	17%
Mexico	86%	14%
Brazil	84%	16%

Concern with Long-term Impact



	Very	Some-what	Not
US	15%	67%	18%
UK	21%	73%	6%
Germany	41%	39%	20%
Hong Kong	36%	56%	7%
Malaysia	73%	26%	2%
Mexico	51%	45%	4%
Brazil	78%	19%	3%

How much
customer friction
will Millennials
tolerate?

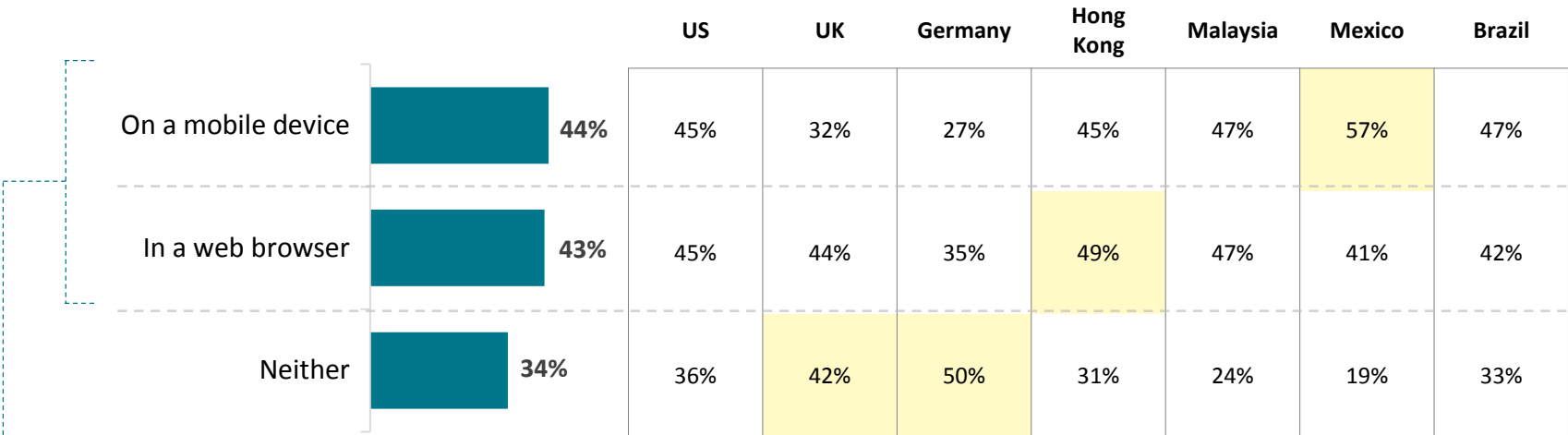


The convenience of storing credentials on a mobile device or in a browser is not a concern for all Millennials.

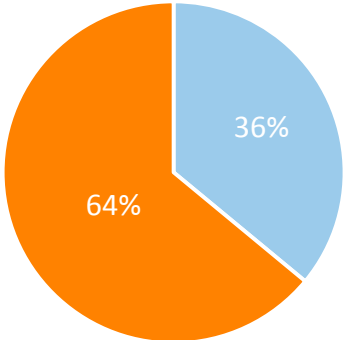
UK and German Millennials are less likely than others to seek the convenience of storing credentials on a mobile device or in a browser.

They, along with US Millennials, are also less likely to use a password manager.

How Login Credentials are Stored



Use of Password Manager



	US	UK	Germany	Hong Kong	Malaysia	Mexico	Brazil
Yes	22%	25%	32%	46%	59%	46%	51%
No	78%	75%	68%	54%	41%	54%	49%

 = higher than other countries

Different countries have different ways of conducting activities, depending on their perceived risk levels.

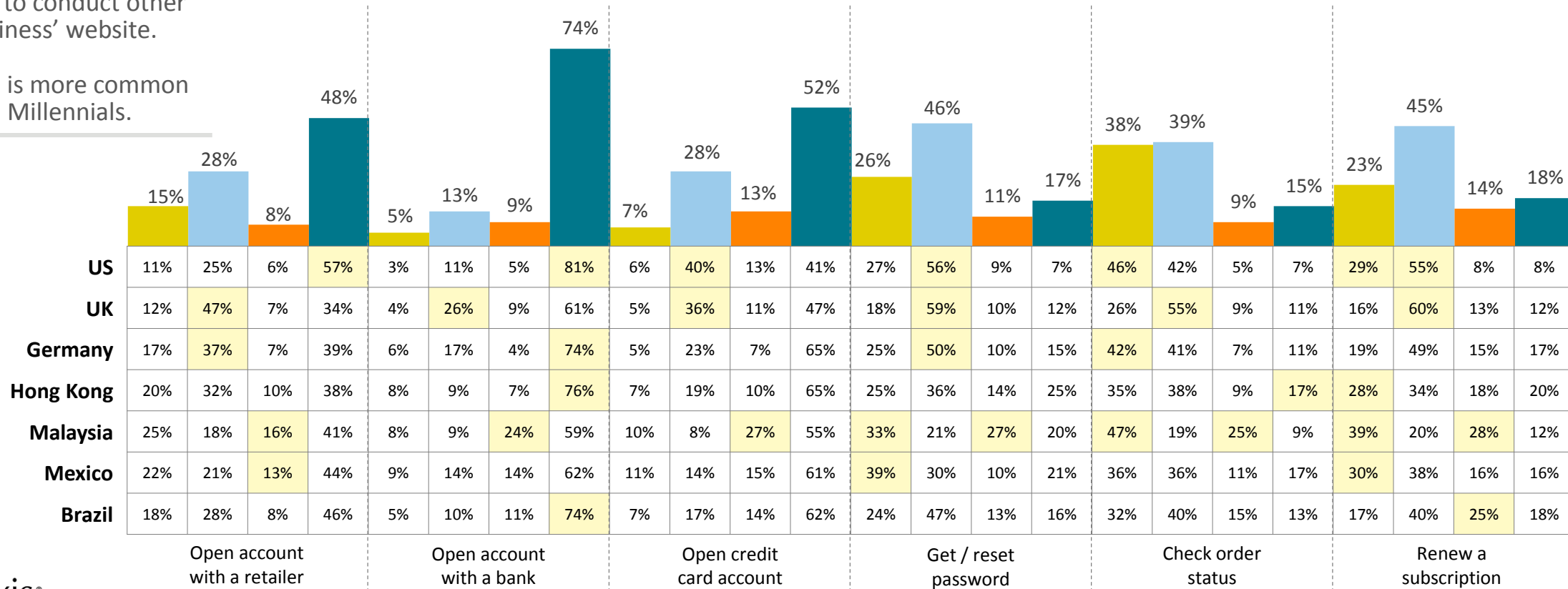
Activities that involve higher risk, such as opening a bank account, are more likely to be conducted in-person, particularly in the US, Germany, Hong Kong, and Brazil.

US, UK, and German Millennials are more likely than others to conduct other activities at a business' website.

Calling a business is more common among Malaysian Millennials.

Ways in Which Activities are Conducted
(among those conducting activities)

- Via Mobile device
- Online at a Business' website
- By Calling the Business
- In-person



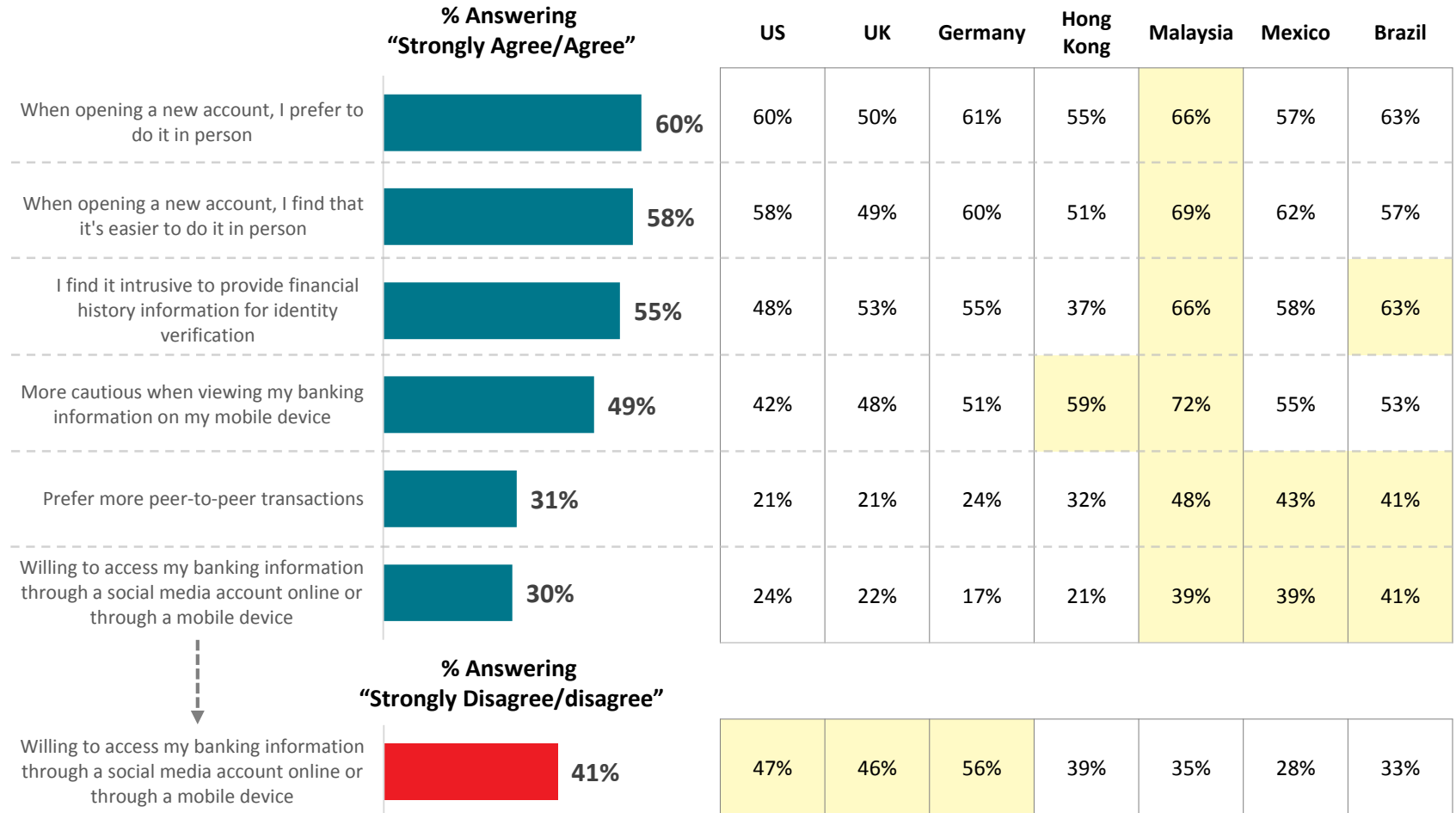
Q: Which of the following activities do you most often conduct via a mobile device, online, phone, or in person?

 = higher than other countries

Concerns with information security and lack of trust with providers drives Millennials to prefer opening accounts in person, particularly in Malaysia.

US, UK, and German Millennials are least willing to access banking information through a social media account.

Willingness to Provide Information for Services



Q: For each statement, please rate your level of agreement.

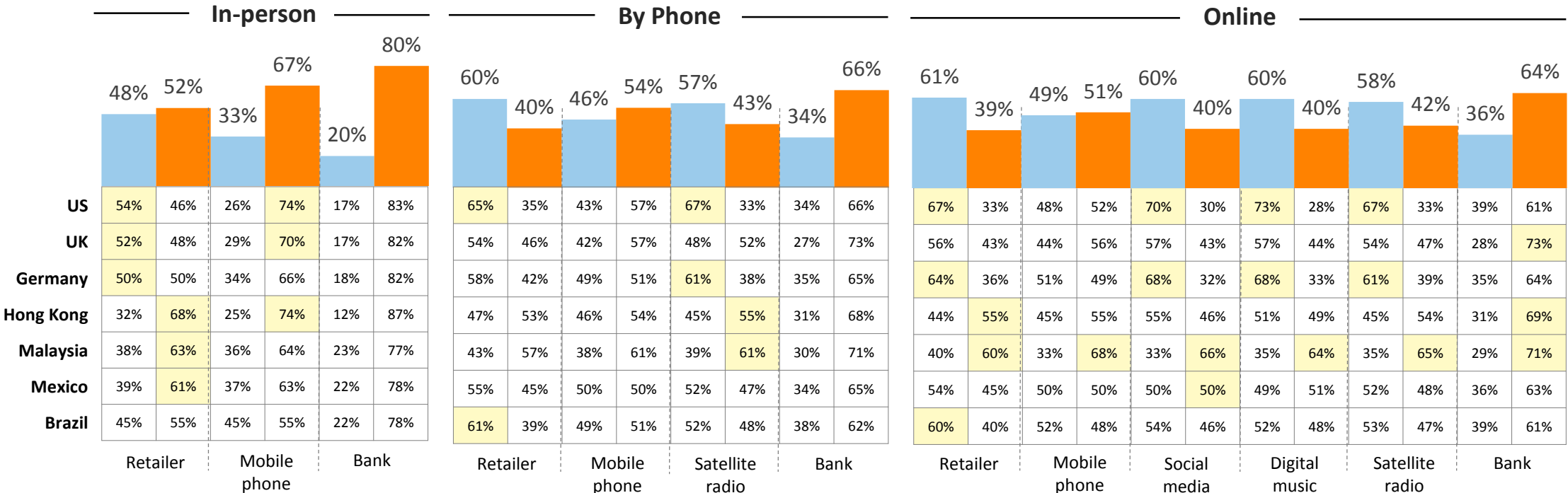
 = higher than other countries

Millennials are similarly willing to spend longer to open a bank account in-person than they are for other accounts via other channels.

US and German Millennials tend to have less patience than others when opening accounts outside of banking, capping their time willingness at 10 minutes. Millennials in Hong Kong, Malaysia, and Mexico are willing to spend longer for most activities.

Time Willing to Spend Opening Account
(among those who would open account by each medium)

■ Up to 10 minutes
■ Up to 15 minutes or more



Reasons to terminate new account opening vary by country.

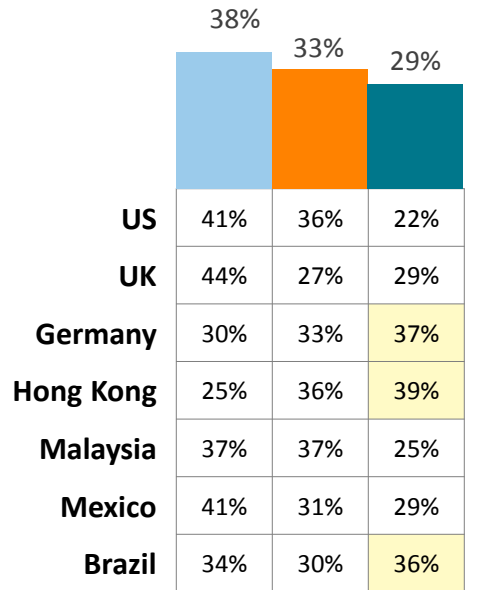
Both amount / type of requested information can cause termination of a new account opening, particularly among US, UK, German, and Hong Kong Millennials

Time is more of a factor for Malaysian, Mexican, and Brazilian Millennials.

UK and Germany are more likely than others to create stand-alone accounts, while most others will link to existing accounts in certain situations.

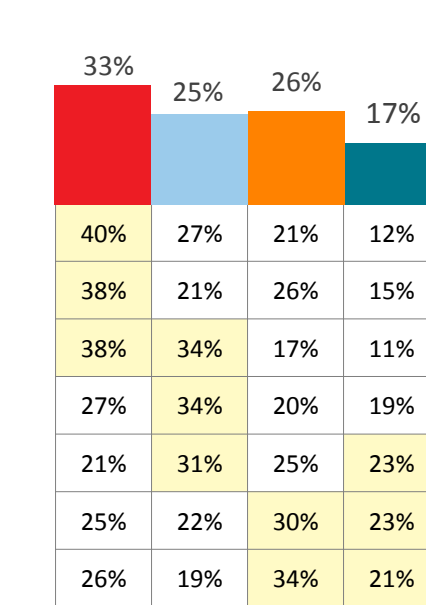
Brazilian Millennials are more likely to link to existing accounts in all situations.

Willingness to Provide Information



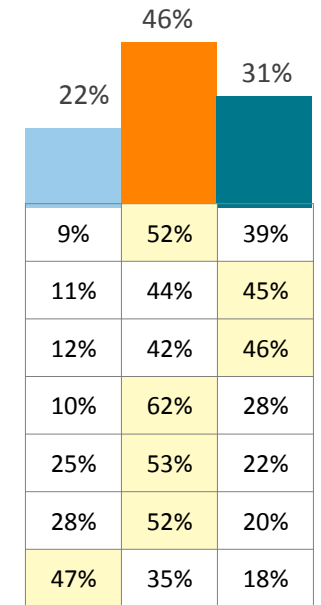
- More when opening account
- More with existing account
- Same amount

What Causes Termination of Account Opening Session?



- Uncomfortable with types of info requested
- Too much info is requested
- Process takes too long
- Too many steps

Link to Existing Accounts
(among those opening online)



- All the time
- In certain situations
- Always create stand-alone accounts


Conclusions




Millennials are very digitally connected in most study markets, though US, Hong Kong, Mexican and Malaysian ones tend to be more power users than others.

- “Power user” means that Millennials in these four markets are using more devices to conduct more transactions than others, including retail shopping, banking and purchasing of online apps.
- US Millennials are also power users of music and video downloads across various devices.
- UK Millennials are more limited than others in terms of device use. And, while Brazilian and German Millennials tend to have as many devices as Millennials in other countries, they are not using as many of them to conduct remote transactions.

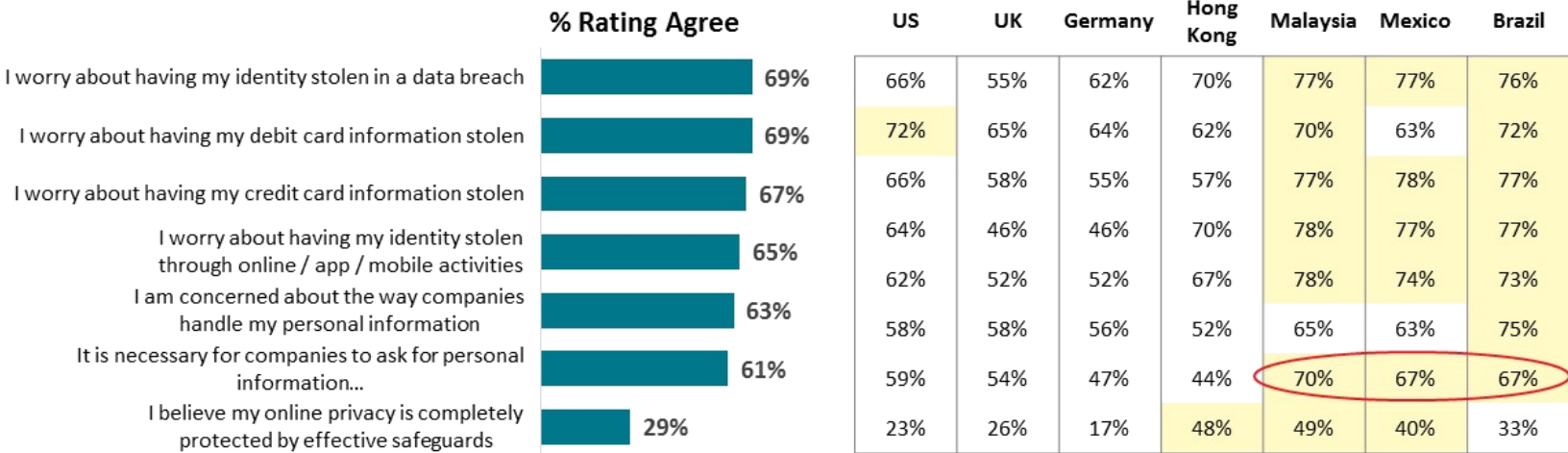
	US	HK	MEX	MALAY	BRA	GER	UK
More Likely to Have Devices	Smartphones	X	X	X	X	X	X
	Laptops	X	X	X	X	X	X
	Desktops		X	X	X	X	
	Tablets	X	X	X	X		X
	Wearables			X		X	
More Likely to Retail Shop with	Smartphones	X	½			½	
	Laptops	X	X	X	X	½	X
	Desktops	X					X
	Tablets						
More Likely to Retail Bank with	Smartphones	X	X		X		
	Laptops	X	X	X	X	X	X
	Desktops	X	X	X	X	X	
	Tablets						
More Likely to Purchase Mobile/Online Apps with	Smartphones	X	X	X	X		
	Laptops		X	X	X		X
	Desktops		X	X		X	
	Tablets				X		
More Likely to Download Music, Videos with	Smartphones	X	X	X			X
	Laptops						
	Desktops	X					
	Tablets	X					

 = Higher than other countries

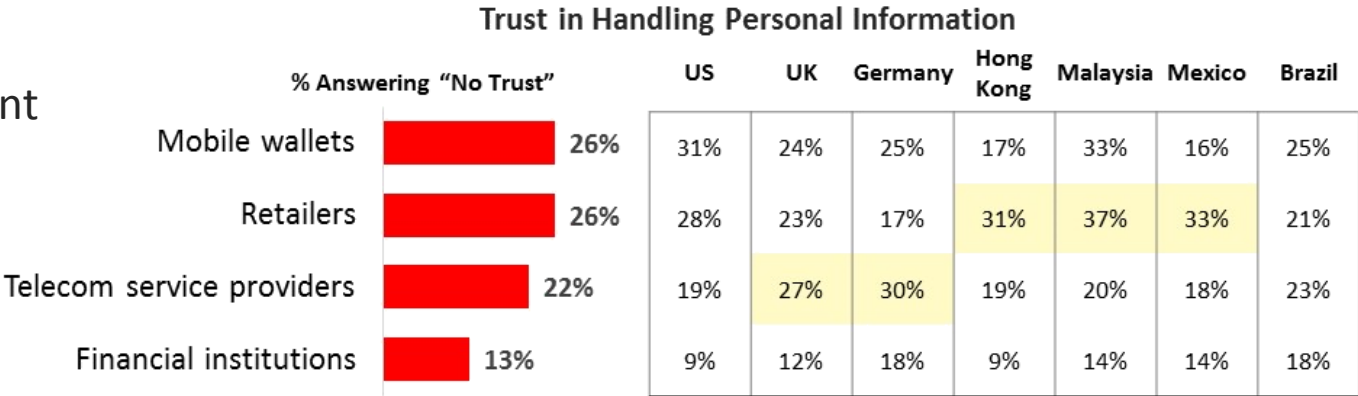
 = More digitally connected or using more devices (power using)

But regardless of being a “power user”, Millennials across markets are similar in terms of having concerns about online / mobile security, a breach of their personal information and provider handling of it.

- While concerns about identity theft and payment information breaches from remote transactions is more heightened among Mexican, Malaysian and Brazilian Millennials, this is a concern for the majority of Millennials in other study markets as well.



- And, there is consistent lack of trust with financial, retail, communications and payment provider companies use of Millennial’s information across study markets.



And, Millennials are similar across markets in terms of exhibiting a disconnect between their attitudes and behaviors towards identity protection and willingness to help companies protect them.

- One notable difference, though, is that German and Hong Kong Millennials are less likely to feel that companies actually need their personal information in order to protect their identities.

	Attitude	Behavior	US	UK	GER	MEX	BRA	HK	MALAY
On one hand, they are consistent with . . .	Having concerns that companies have too much of their personal information and . . .	Will terminate opening a new account if too much sensitive PII is asked.	X	X	X	X	X	X	X
	Having concerns about their data being compromised through data breaches and . . .	Being reluctant to share sensitive personally identifiable information with companies.	X	X	X	X	X	X	X
On the other hand, they are inconsistent with . . .	Being worried about having their debit or credit card information stolen, yet . . .	Use these cards to make remote purchases directly with the provider.	X	X	X	X	X	X	X
	Being worried about having their identity stolen through online/app-based/mobile activities, yet . . .	Use online or mobile browsing for purchases and financial transactions.	X	X	X	X	X	X	X
	Realizing that companies need to ask for their information to protect them from identity theft and fraud, yet . . .	Think twice before actually providing that information or will terminate if too sensitive	X	X		X	X		X

Further, there are similarities across markets in terms of Millennial limits on the amount of friction they will accept to verify identity and prevent fraud.

- Nearly all will terminate opening a new account if they feel that too much sensitive information is being requested.
- Biometrics is used by Millennials in varying degrees across study markets, though largely limited to smartphones. Trust in biometrics is often limited, with the exception being among Mexican and Brazilians.
- Millennials differ in terms of their patience when opening new accounts. US and German Millennials are less patient, while Hong Kong, Malaysian and Mexican ones are more patient. That said, there is commonality across markets in terms of being willing to wait longer when opening a bank account in-person.

As a result, there are many similarities between Millennials across markets in terms of attitudes and behaviors to online / mobile / identity security. Differences are more nuanced than stark.

Similarities

- All are digitally connected to online and mobile devices
- Most tend to own their devices; all use them for both business and personal
- If using biometrics, they tend to do so on their smartphones
- Identity theft, online security and breaching of payment information is a concern to most across countries
- Lack trust in financial services, retail, communications and payment provider organizations to handle their personally identifiable information (PII)
- Limited acceptance of friction
 - Very limited willingness to share their PII
 - Prefer to open bank accounts in person
 - Time and amount of sensitive information can cause them to terminate opening a new account

Nuances

- US, Hong Kong, Mexican and Malaysian Millennials are more “power users” than others
- Different devices used for different types of transactions
- US, Hong Kong, Mexican and Brazilian Millennials use biometrics more than others; Mexicans and Brazilians have more trust in this application
- Malaysians, Mexicans and Brazilians are more sensitive to ID theft, online security and data breaching; while they are more likely to recognize need for companies to have their personal information, they are bothered by it as are others
- Germans and Malaysians are less willing than others to provide PII.
- Opening non-bank accounts online is more comfortable among US, UK and Germany

Stark Differences

- Use different payment methods for remote purchasing
- Different levels of patience when opening new accounts
 - US and German Millennials have less patience
 - Hong Kong, Mexican and Malaysian ones have more patience.

Recommendations



The identity authentication process should be different based on not just the type of transaction experience (in-person, online, by phone), but also accounting for nuanced sensitivities and device use by market.

- Not all transactions have the same risk level, nor are perceived the same among different Millennials.
 - ❑ Risk levels vary by channel (i.e., in-person versus mobile), value (i.e., high value vs. commodities) and device (online versus mobile). The same devices are not used consistently across markets by Millennials; US, Mexican, Hong Kong and Malaysian Millennials use more devices for more things and are therefore more exposed to risk.
- At the same time, Millennials differ in terms of patience and sensitivity towards managing this risk.
 - ❑ Patience levels for identity validation vary; companies may lose US and German Millennials if they have to wait too long.
 - ❑ Sensitivity around identity theft and protection varies: Malaysians, Mexicans and Brazilians are most sensitive about these issues, though have a similar discomfort as others with regard to providing information to verify identities. This makes them even more sensitive.
 - ❑ Therefore, the authentication process needs to have flexibility across markets to ensure the optimal customer experience based on those in-country nuances. Companies will need to minimize friction by adjusting the degree to which they ask for / use customer information across different transactions (i.e., pick their battles).

Let LexisNexis® Risk Solutions help you adjust your authentication flow based on risk profiles, so that you can focus on delivering the right customer experience every time.

It will be important to limit the amount of PII that is requested of Millennials for identity protection, particularly among Germans, Malaysians, Mexicans and Brazilians.

- Requests for too much or too sensitive information can be a deal-breaker for Millennials across markets, but it could happen more quickly and easily among those who are most sensitive to identity theft and company PII handling.
 - ❑ Even though they recognize the need for companies to have their personal information, the lack of trust with how companies handle it could become a barrier to their willingness to provide sensitive information.
 - ❑ To the degree available, pre-populated data could reduce this challenge.
 - ❑ Enabling access to existing accounts through one-time passwords is acceptable to Millennials except for Malaysians and Germans.
 - ❑ Biometrics is an additional option to reduce friction, particularly among US, Hong Kong, Mexican, and Brazilian Millennials. It could be an option with others to the degree there is more transparency around the types of personal information that Millennials need to give (or education that they can provide less information and still get the same or better identity protection).

Let LexisNexis® Risk Solutions tailor the authentication experience with a layered approach, such as One Time Password with Knowledge Based Authentication or with Biometrics linked to other identity proofing solutions. These will help detect true fraud that reduces customer friction and ensures customer loyalty.

To further lessen friction, companies will need to supplement their information with data from external providers who specialize in identity verification / validation.

- As noted, it will be challenging for companies to gather much data from Millennials which would prove useful towards developing a complete profile of them.
- As a result, reliance on more robust external data – including the underserved / underbanked – will be essential to developing profiles of these customers.

Let LexisNexis® Risk Solutions provide richer and more accurate profiles of consumers than you can get from other solutions in the market today. This includes giving you more information on the underserved / underbanked population (inclusive of a large portion of millennials with a limited credit footprint).



LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. Other products or services are the trademarks or registered trademarks of their respective owners. Copyright © 2016 LexisNexis.

About us

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of RELX Group, plc, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.