



LexisNexis® Risk Solutions
German Millennial Study
Privacy vs. Customer Experience



LexisNexis®
RISK SOLUTIONS

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 401 Millennials, deployed during April-May 2016.
- Respondents represented both younger (18-24 years old) and older (25-34 years old) Millennials across Germany.
- The overall margin of sampling error is +/- 4.89% at the 95% confidence level.
- Data reflects the German Millennials population based on weighting to the German Census.



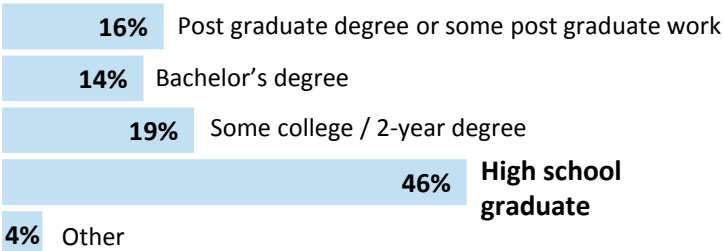
Who are Millennials?



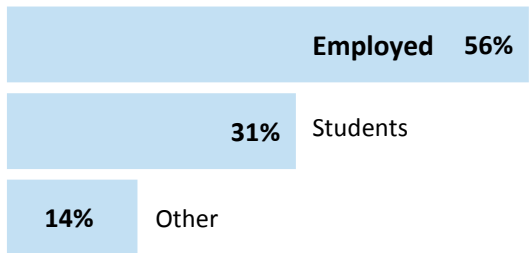
German Millennials are diverse in terms of occupation; the majority work in non-professional jobs with many having only a high school equivalent education. Over one-third are still living with their parents.



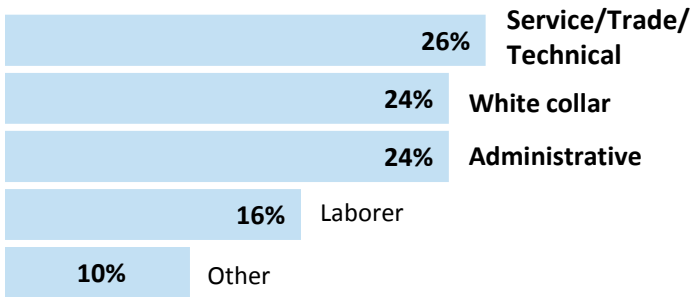
Education Level



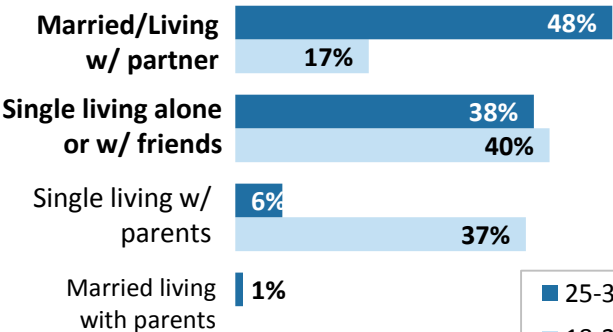
Employment Status



Occupation



Relationship Status

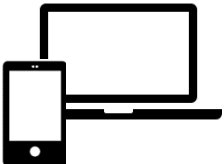


Use of Financial Services



81% use traditional banks

While 50% also use online-only banks



Inside the Millennial mind



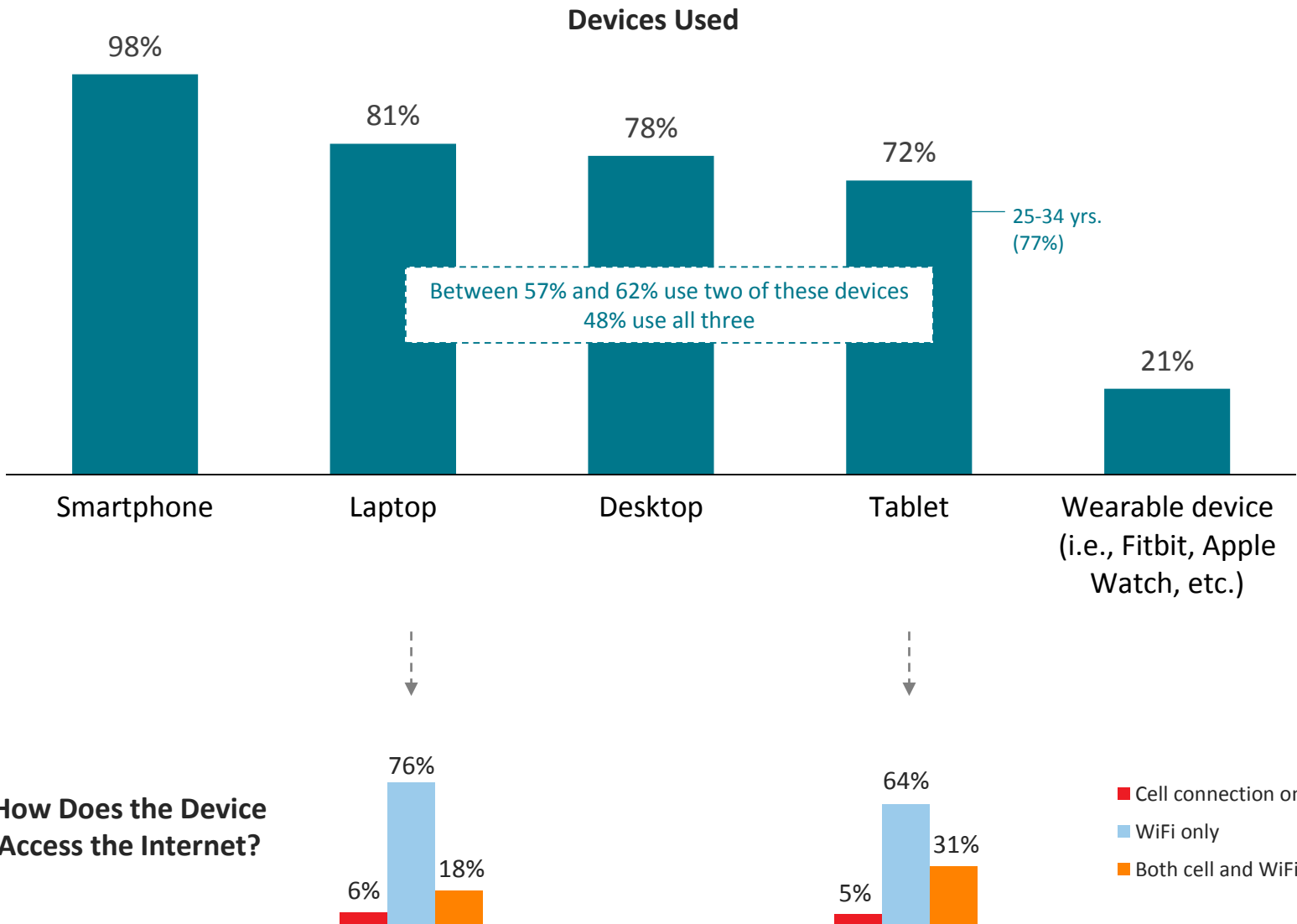
German Millennials are digitally connected through multiple devices.

German Millennials use an average of **3.5 different types of devices**, including a smartphone plus some combination of a laptop / desktop computer / tablet.

Tablet use is more prevalent among older German Millennials (77% among 25-34 years old).

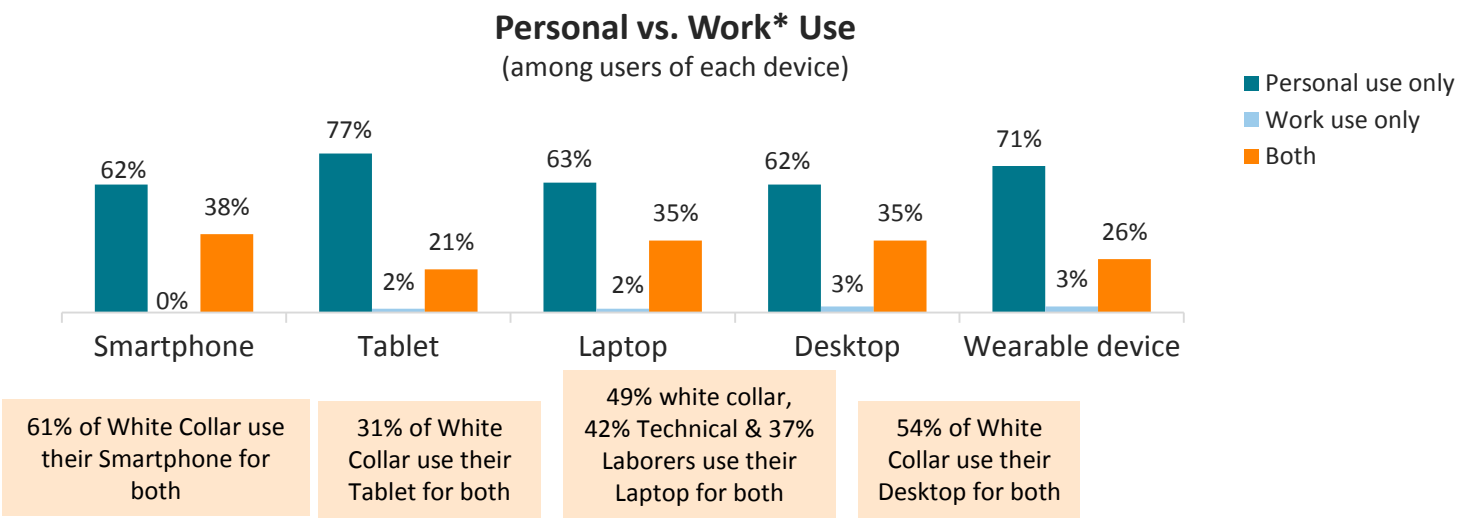
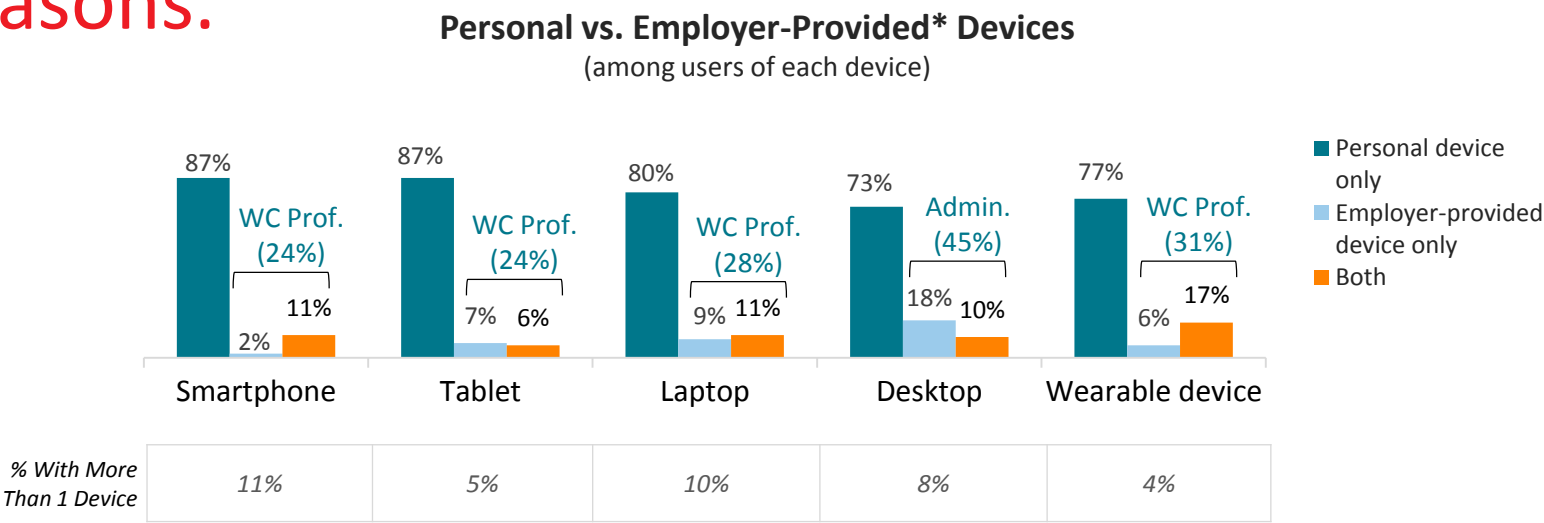
Wearable device use is very limited, most often to those with higher incomes (32% among \$75K+) and education (32% among Post-Grad).

WiFi is predominately used to access the Internet on laptops and tablets, though a sizeable minority also use a cellular connection in addition to WiFi for their tablet.



Most of these devices are personal (not provided by an employer), with a number of White Collar professionals using them for both business and personal reasons.

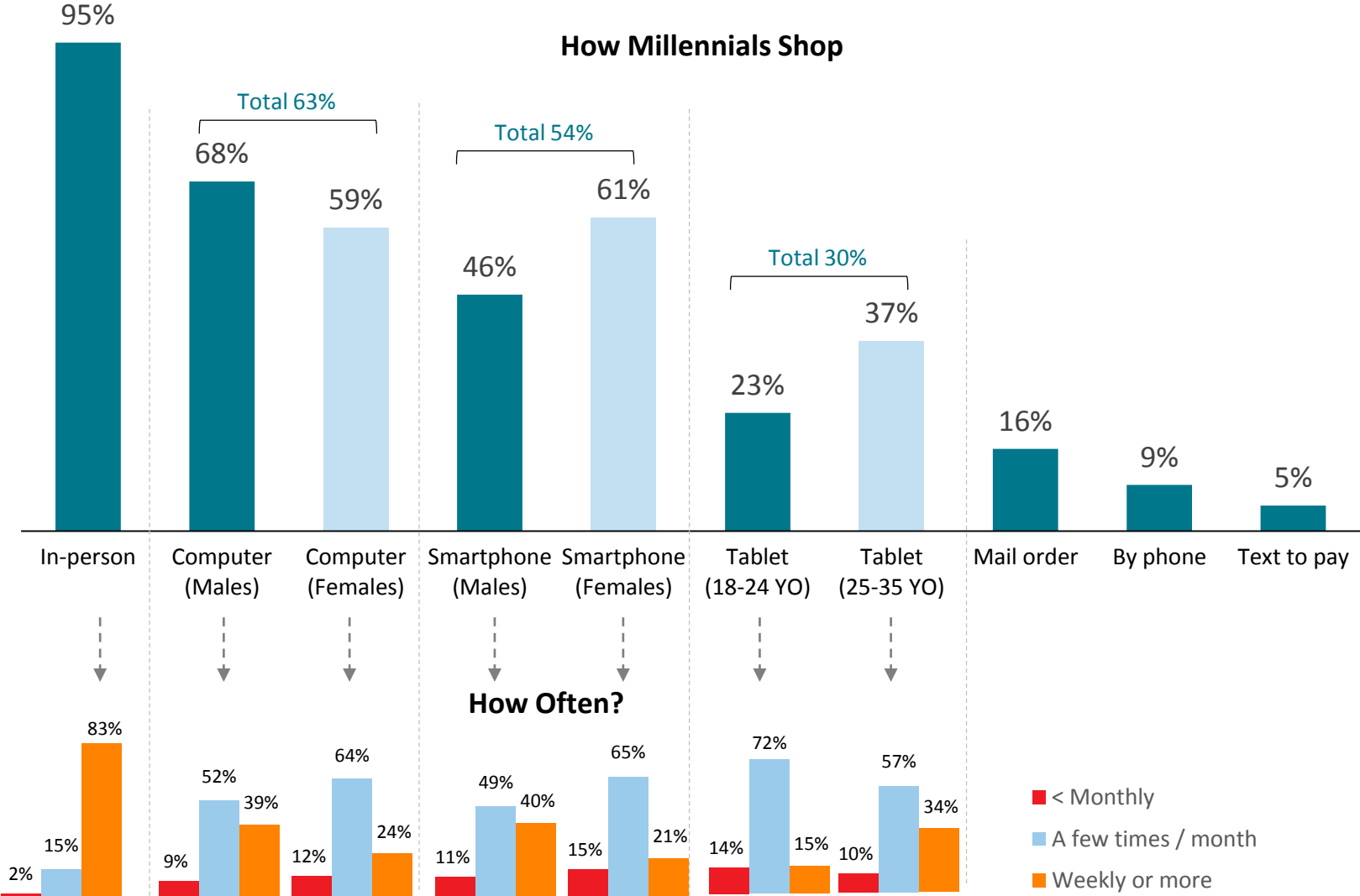
To the degree that devices are purchased by an employer, this occurs more often among White Collar professionals than others. But there is still a number of professionals who use their own devices for business along with personal. This more often includes personal smartphones, laptops, and desktop computers.



In-person shopping is most common and frequent among German Millennials, though they also do remote shopping too.

German Millennials are somewhat split between using the computer or smartphone for remote shopping, while tablet use is still limited for purchases – particularly among the younger half.

Female Millennials are more likely than males to embrace mCommerce via their smartphones.



In-store purchasing is not driven by concerns around online security, but rather the immediacy of experiencing and getting products in real-time.

German Millennials are driven to the store based on traditional reasons of being able to see, touch and try merchandise, as well as to take it home the same day.

Concerns with online provider credibility and security are *not* driving German Millennials to the store.



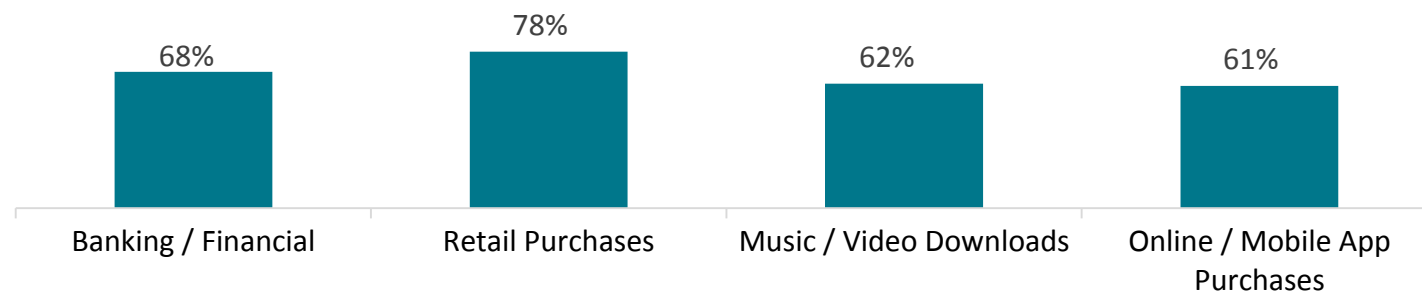
Along with purchasing, German Millennials also conduct remote banking – but use more established remote channels to do so.

Retail purchases are commonly made across device types, but banking is more limited to computers / online browsers than the mobile channel options.

This suggests less confidence in the security of mobile browsers for very sensitive transactions.

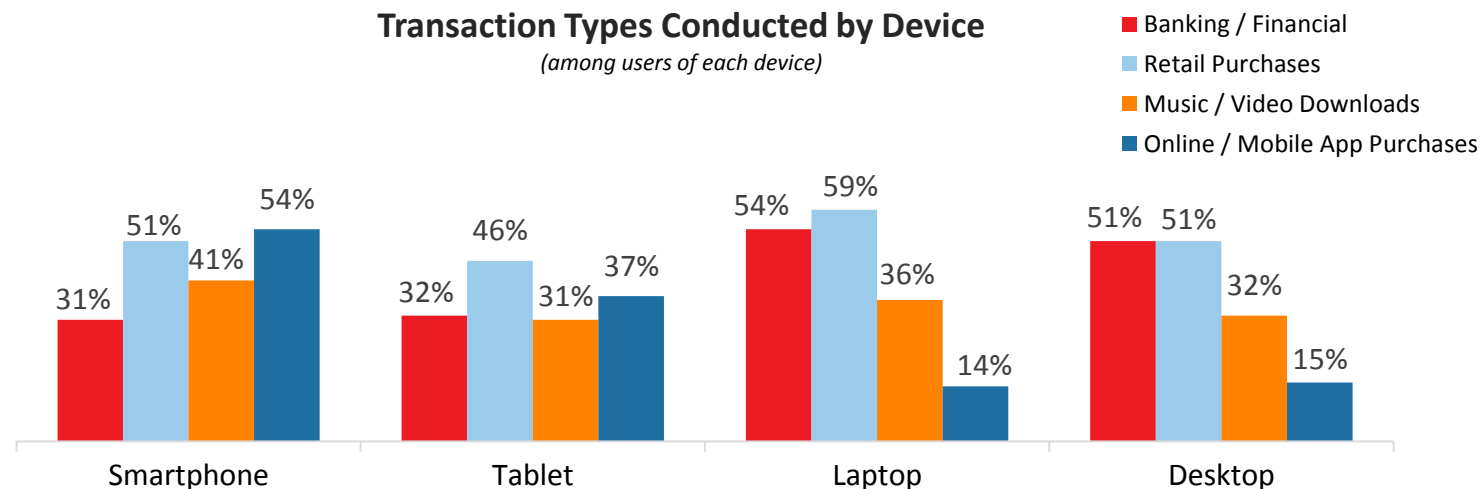
Transaction Types Conducted Remotely

(among users of each device)



Transaction Types Conducted by Device

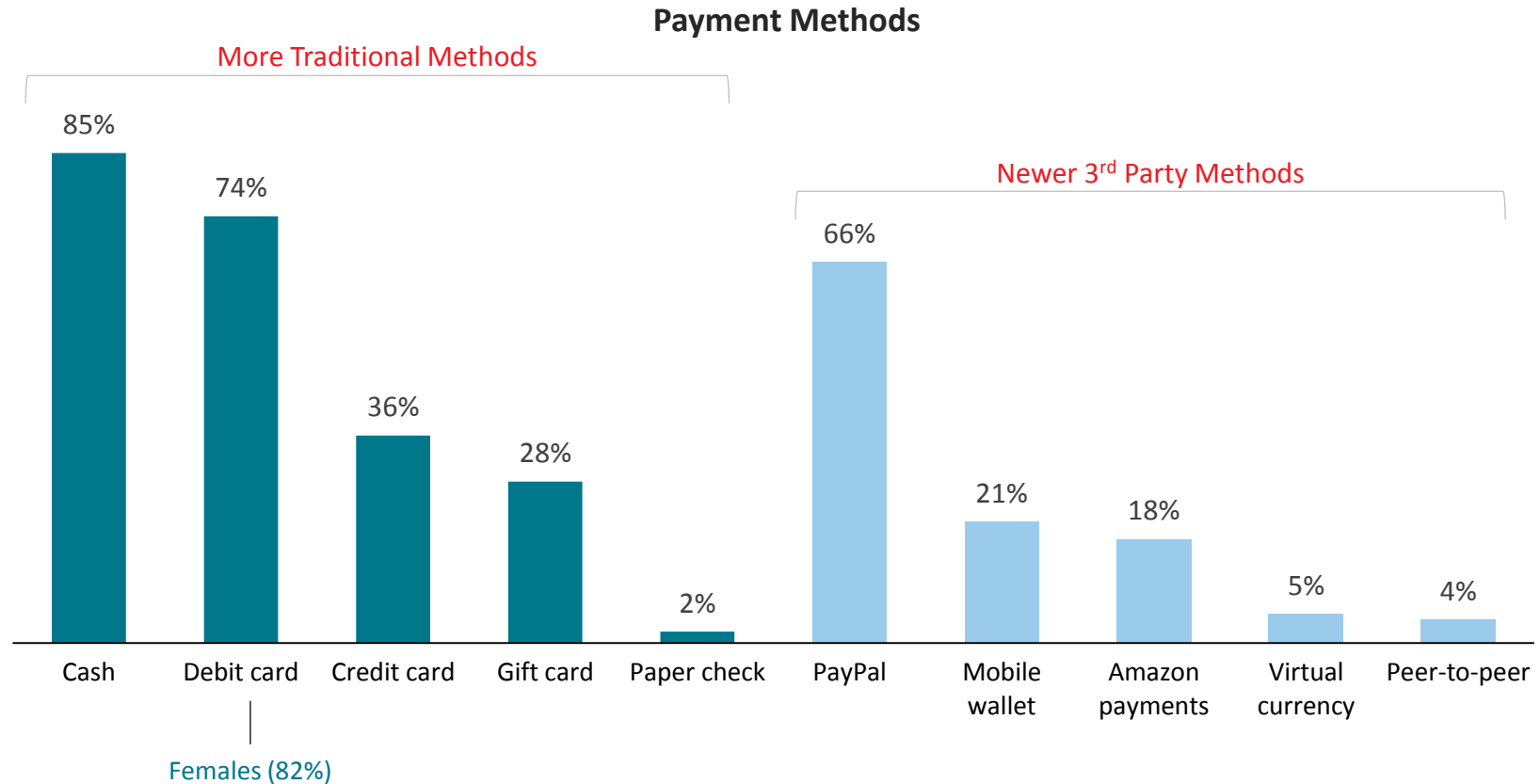
(among users of each device)



Along with cash, German Millennials use both direct-to-provider and 3rd party payment methods, particularly debit cards and PayPal.

Credit card use is significantly smaller among German Millennials, as are other 3rd party payment options beyond PayPal.

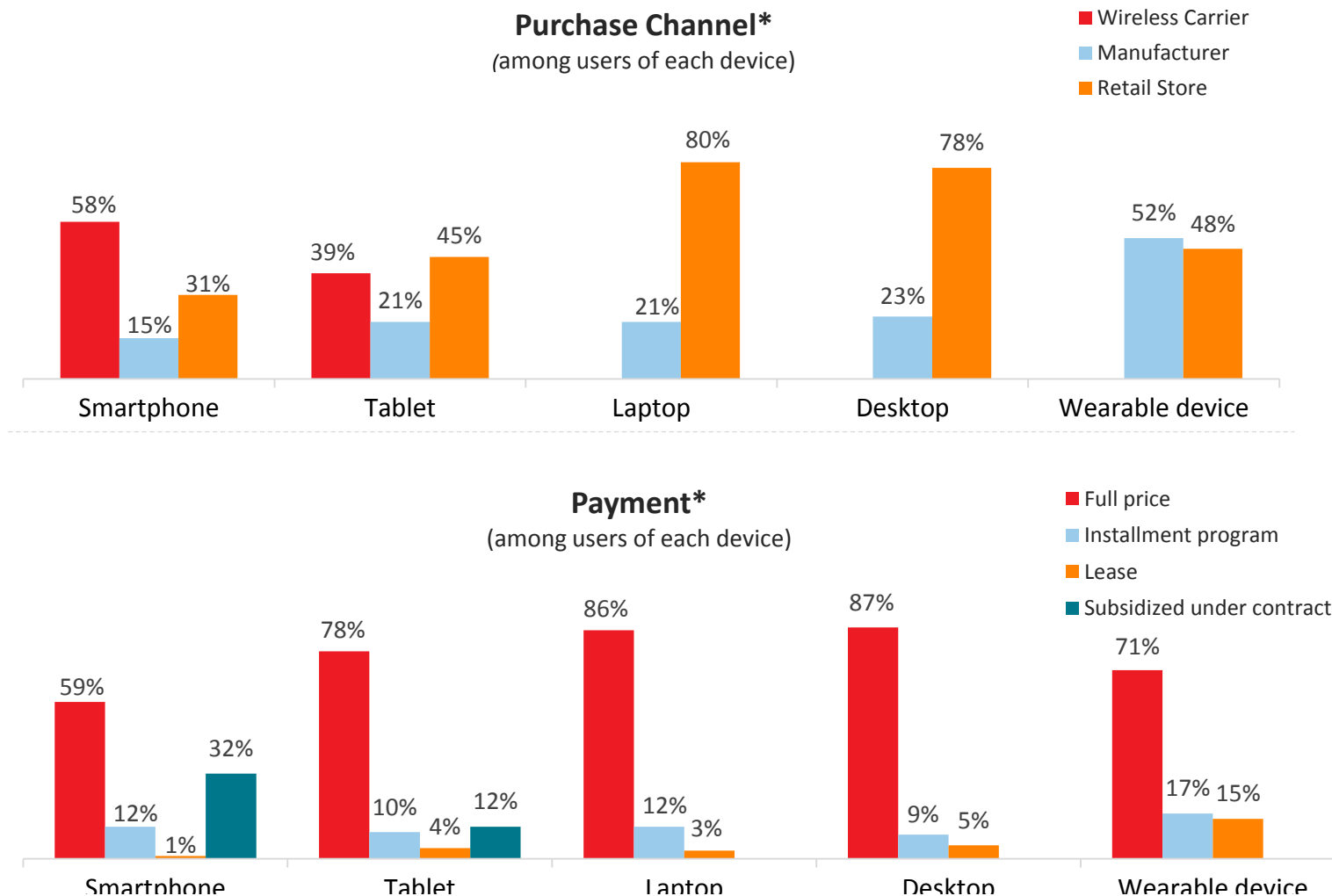
While debit card use is prevalent across gender, female Millennials rely on this even more than their male counterparts (82% vs. 67%)



Point of purchase varies by device, with retailers as the primary channel for computers and carriers as the one for smartphones.

Devices are generally paid at full price regardless of provider type, with some exception regarding smartphones. As in North America, the wireless carriers are involved in the purchase process given that phones operate over their networks. Therefore, they will offer different payment methods as incentives for generating new and retaining current subscribers.

Since just over one-third of tablet users reported using cell connections, this would explain wireless carriers as a point of purchasing among some.

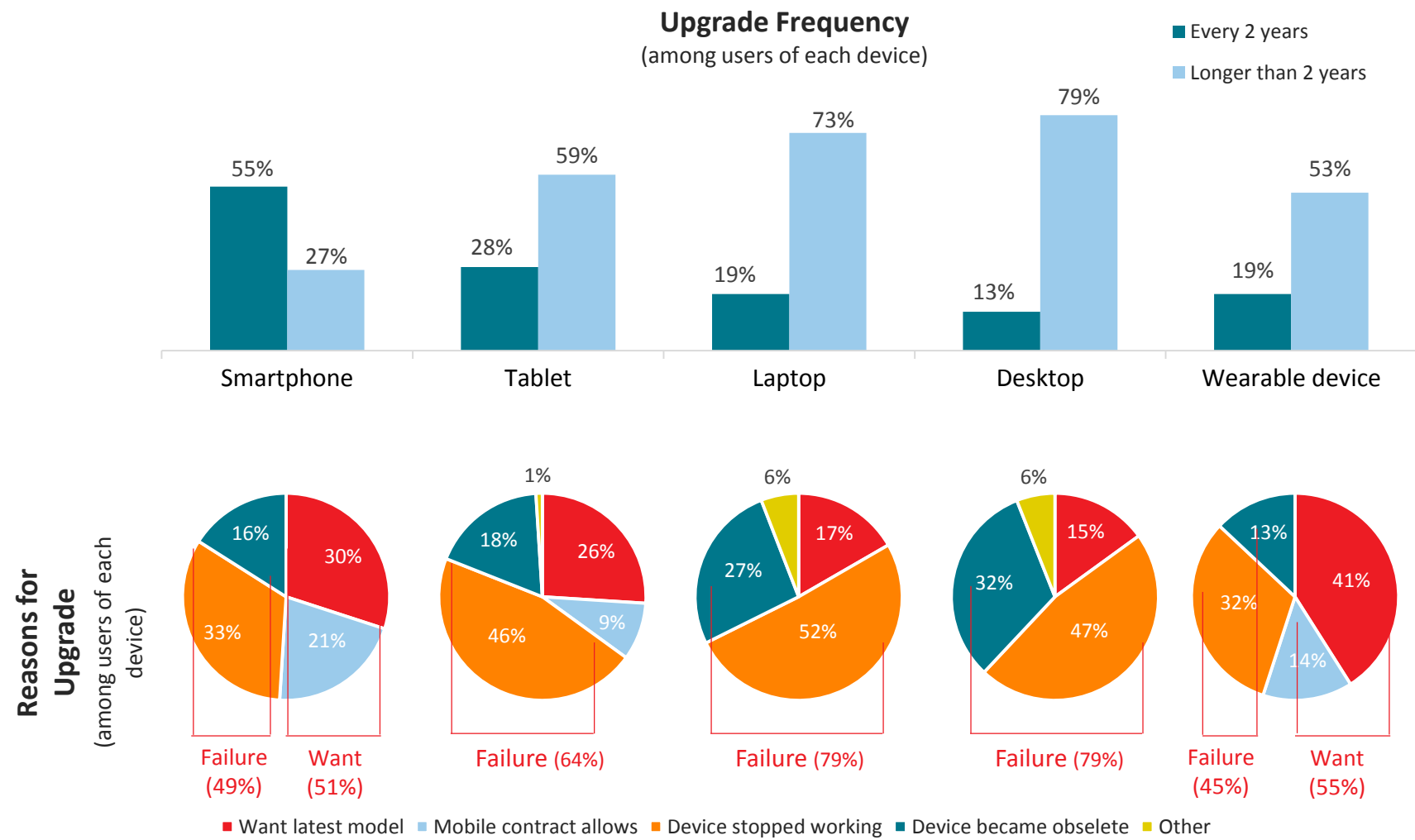


Smartphones are most often upgraded within every 2 years while other devices are used for longer periods of time.

Millennials are mixed between upgrading based on want/being provided the latest model and circumstances where the device stops functioning.

Tablets, laptops, and desktops tend to be used until their functionality fails.

Some like to have the latest and greatest wearable devices, though appear willing to wait longer for such replacements.



Is trust an issue?



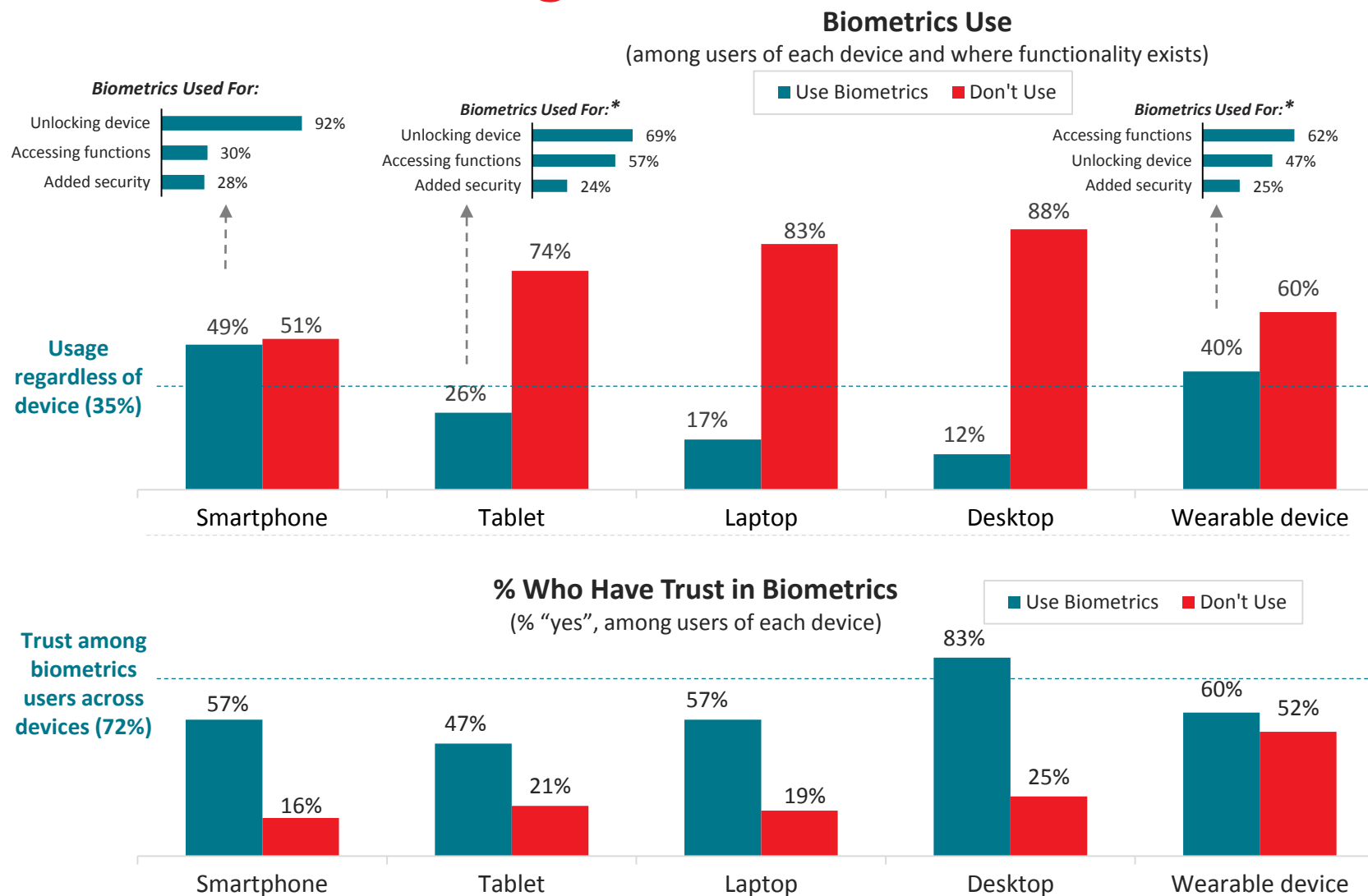
There is some use of biometrics among German Millennials with smartphones and wearable devices, though with mixed levels of trust.

Biometrics use is generally limited to smartphones and wearable devices. **With smartphones, biometrics is generally used to unlock the device, while it's less often viewed as an additional security feature across devices.**

Over one-quarter to tablet users are also using biometrics.

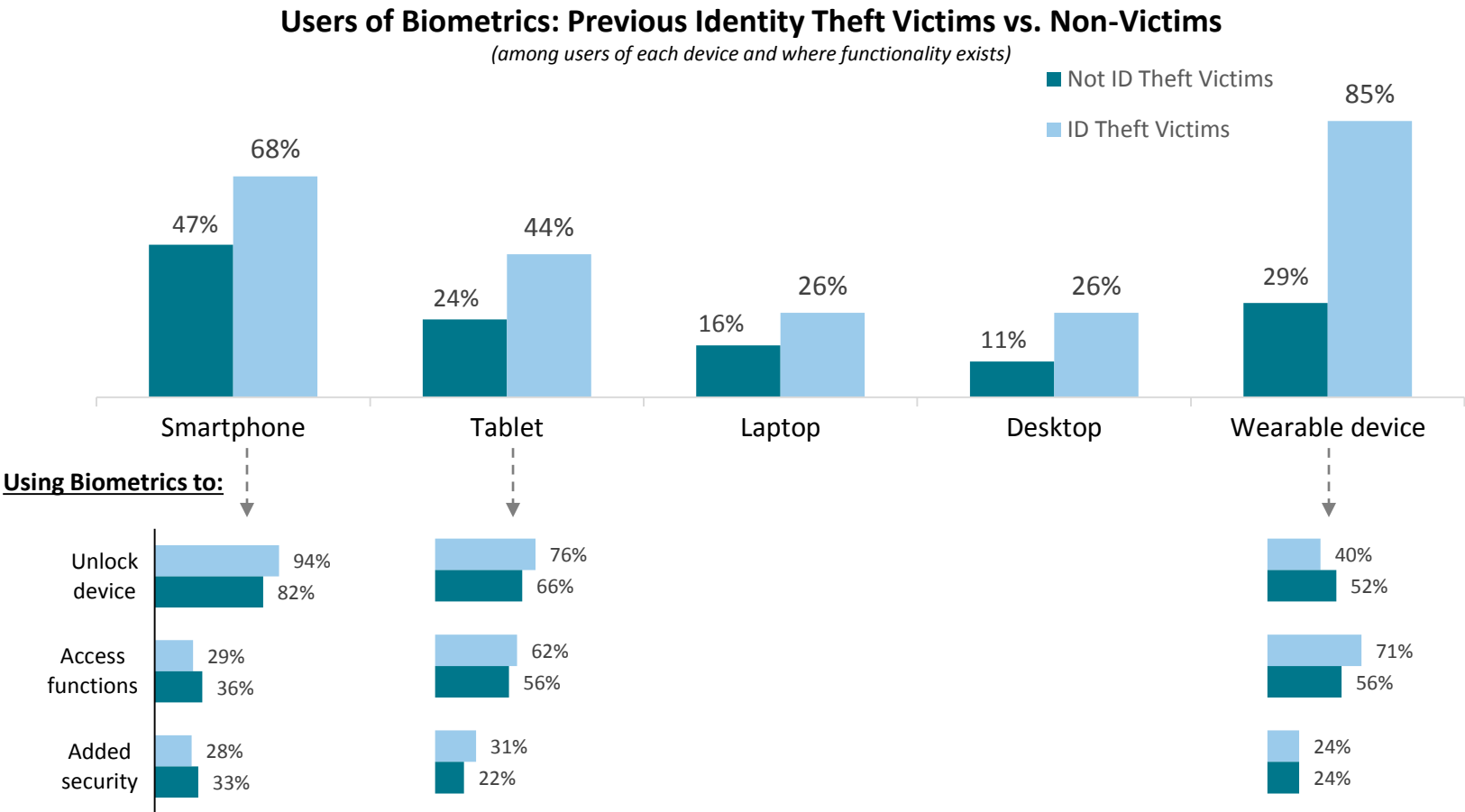
Not surprisingly, those who aren't using biometrics do not have full trust in the security measure.

And even those who are using biometrics have **somewhat mixed** feelings.



Previous identity theft victims are more likely than others to use biometrics on their smartphone, tablet, and wearable devices.

However, there is no difference between previous identity theft victims and others in terms of reasoning for biometrics use – to unlock the device and / or access functions. Added security is not a driver or differentiator among identity theft victims’ use of biometrics.



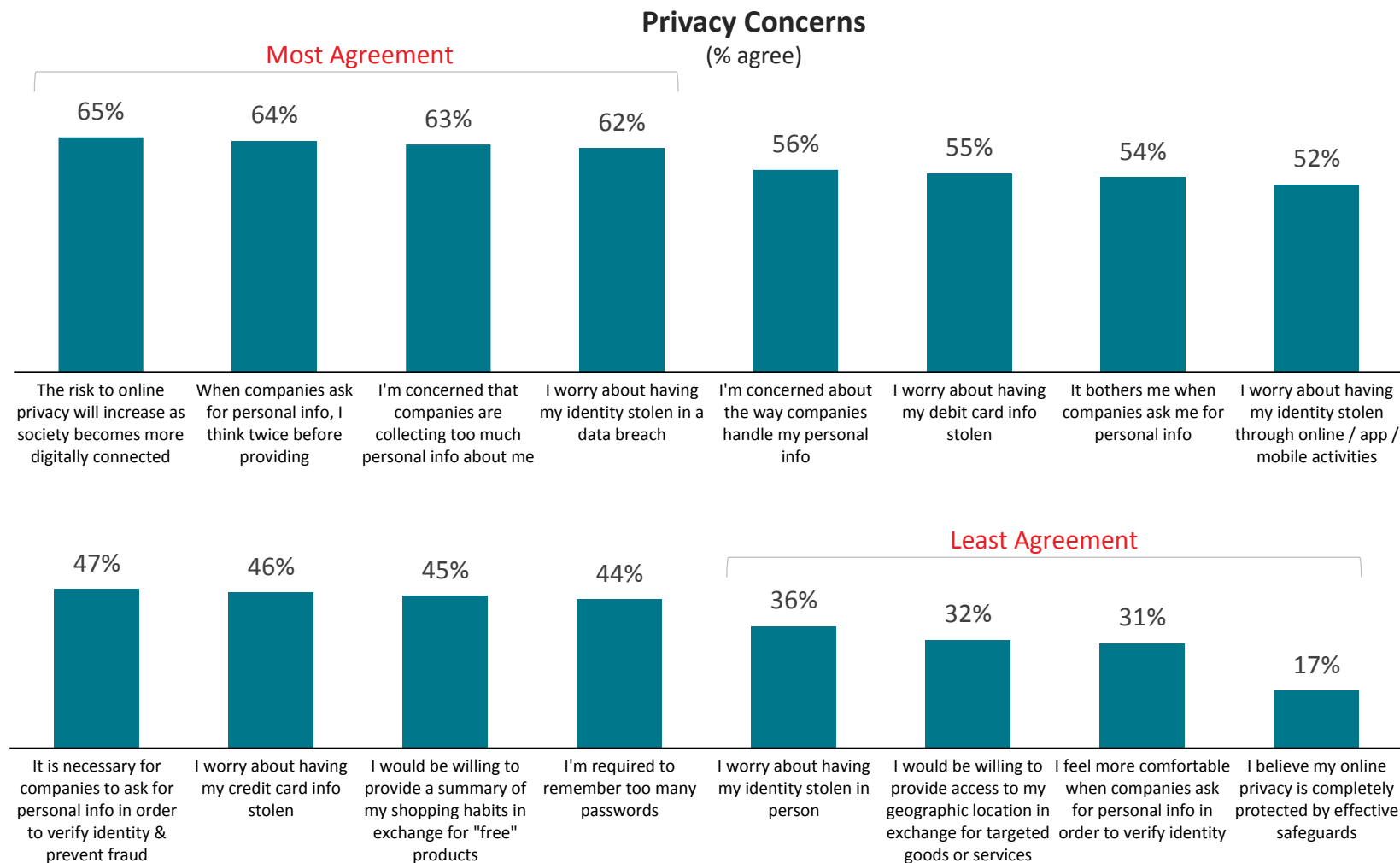
German Millennials worry about online security but are sensitive to giving personal information to companies that can protect identities.

Top concerns relate to the risk of privacy and identity security, along with giving too much personal information to companies. There is a lack of trust in how such companies might handle Millennials information.

Much of this worry is related to distrust in current safeguards used by companies as they collect information to verify identity.

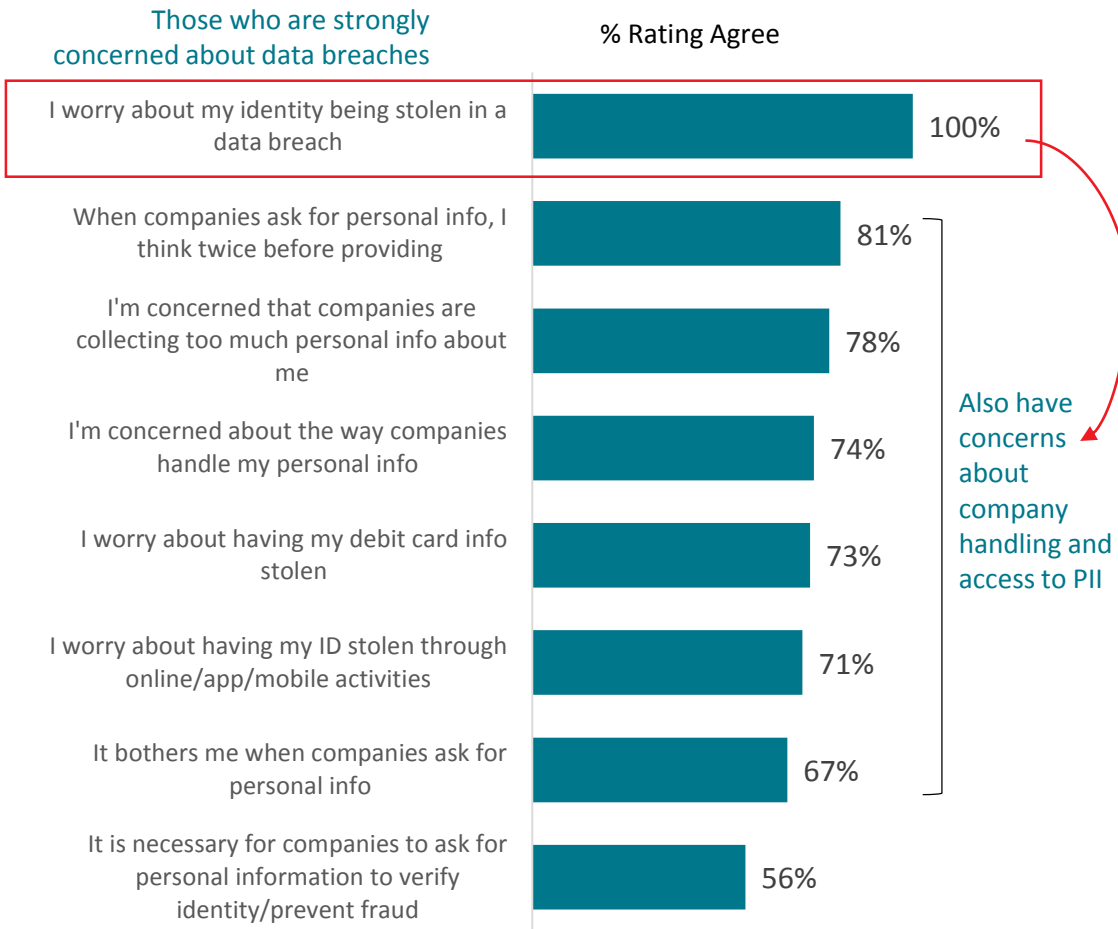
Given such distrust, less than half are even willing to provide information in exchange for freebies – and even fewer are willing to provide their geographic location for goods and services.

While German Millennials are making purchases remotely, using their debit cards, they have concerns about having this data breached and having their identities stolen through online / mobile activities.



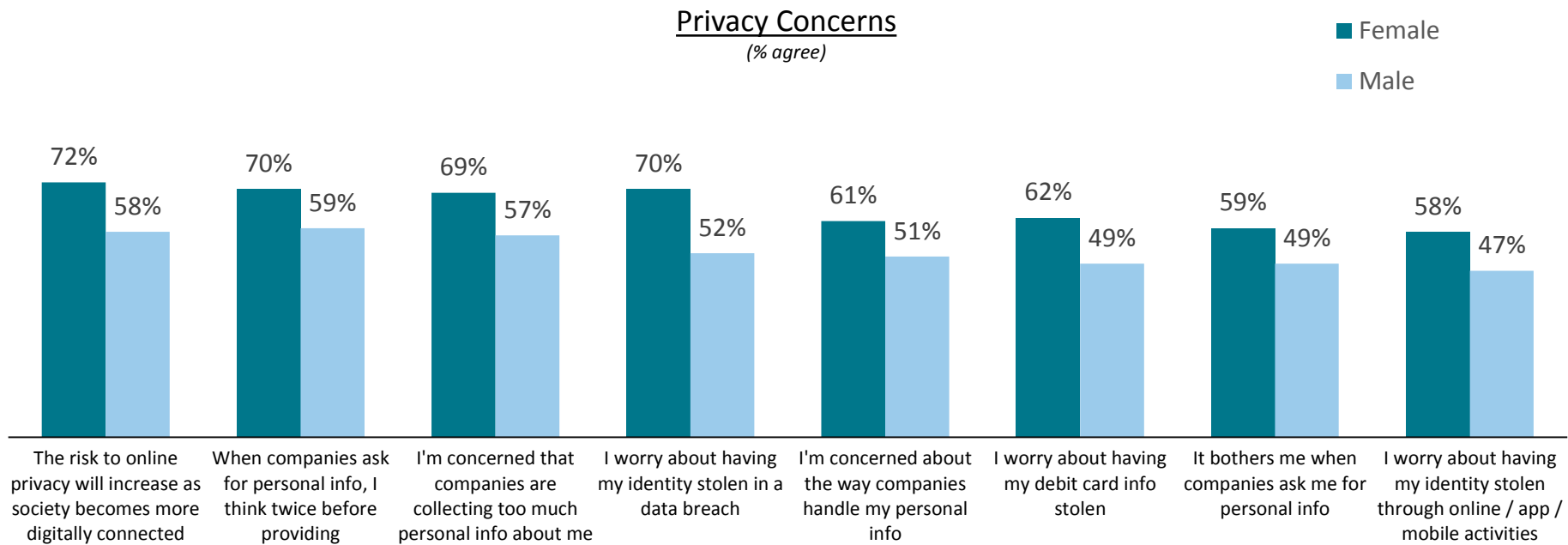
Those concerned with having their identity stolen in a data breach are more likely to be worried about companies having and using their personal information.

Two-thirds or more of those who are worried about having their identity stolen through a breach also have concerns about companies having too much PII and ways in which this may be handled. That said, at least half recognize that companies need their information in order to verify identities and prevent fraud.



Female Millennials are significantly more worried than males about privacy, identity protection and use of their information by others.

This doesn't mean that these are not concerns of males; nearly half or more state the same fears. However, these concerns are more heightened among females.

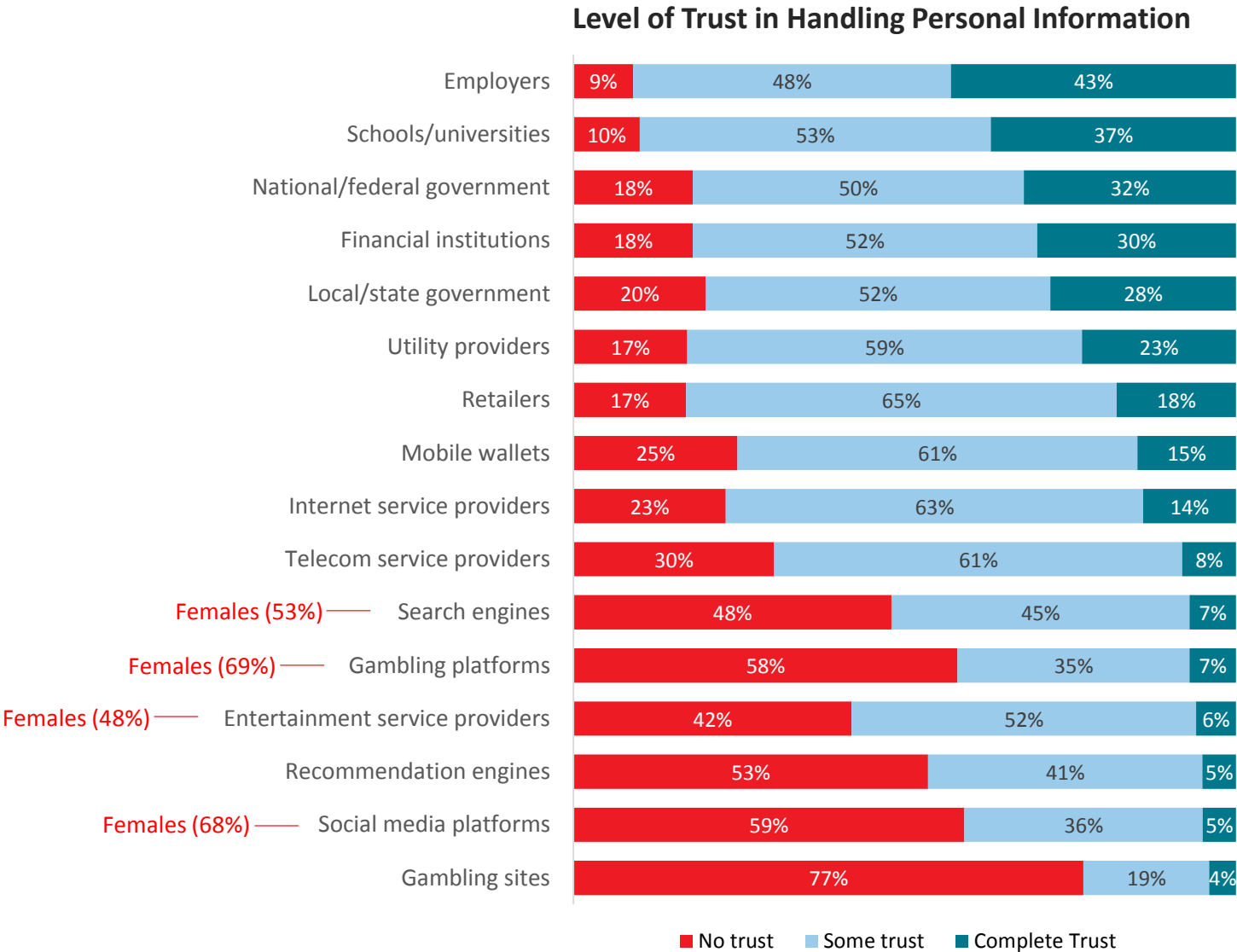


There is lukewarm trust in many providers with regard to handling Millennials' personal information.

Even though there is more trust in Financial institutions than others, they too are not fully trusted.

Communications companies, payment providers, and retailers are trusted even less.

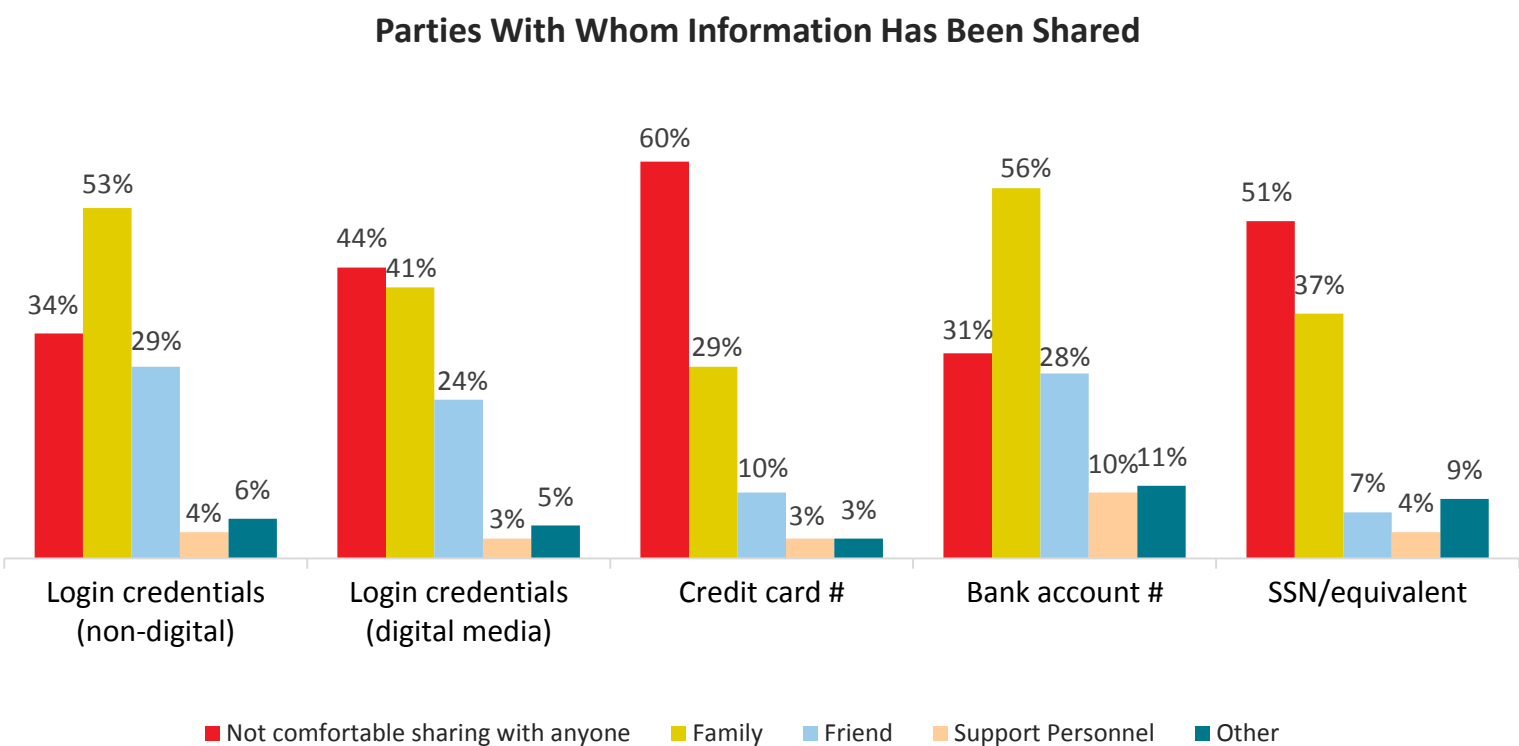
The difference between genders occurs most with online / remote providers as well as those in the Entertainment industry, with females being less trusting.



German Millennials are careful about sharing information outside of trusted family members.

Nearly half or more have shared such sensitive data as bank account number, SSN equivalent and login credentials with family members.

German Millennials don't tend to share this information with friends, support personnel and others, with a number who are uncomfortable sharing this with anyone including family.

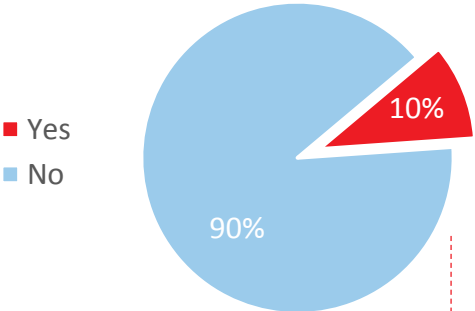


Only a small minority of German Millennials report having been victims of identity theft.

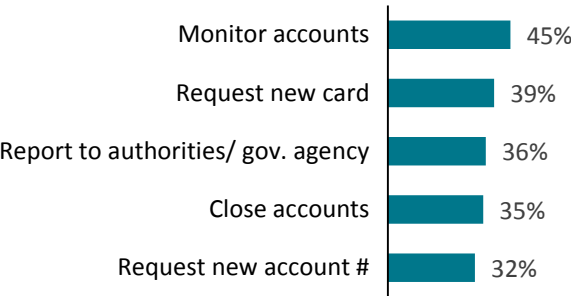
Those who've been victims of identity theft have varied in the actions they took to resolve it.

Only half began to keep passwords private for future protection, even though a significant majority are worried about the long term impacts of this identity breach.

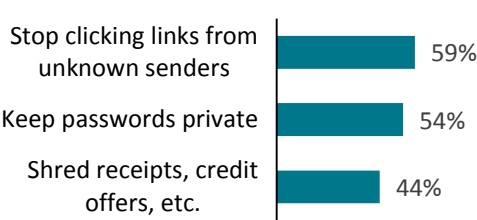
Victim of Identity Theft



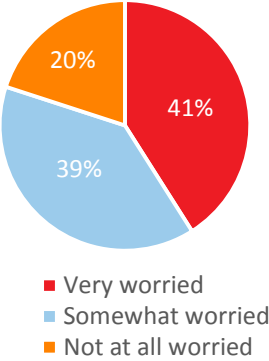
Actions Taken to Resolve



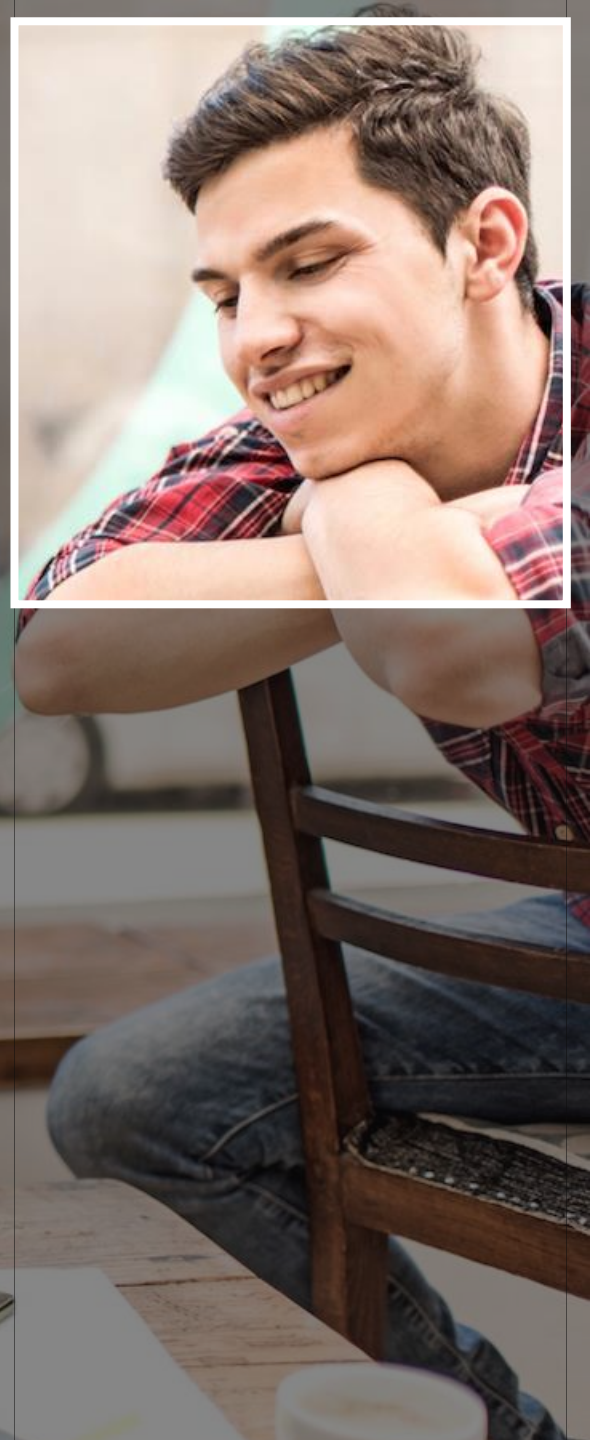
Steps to Protect Identity in Future



Concern with Long-term Impact

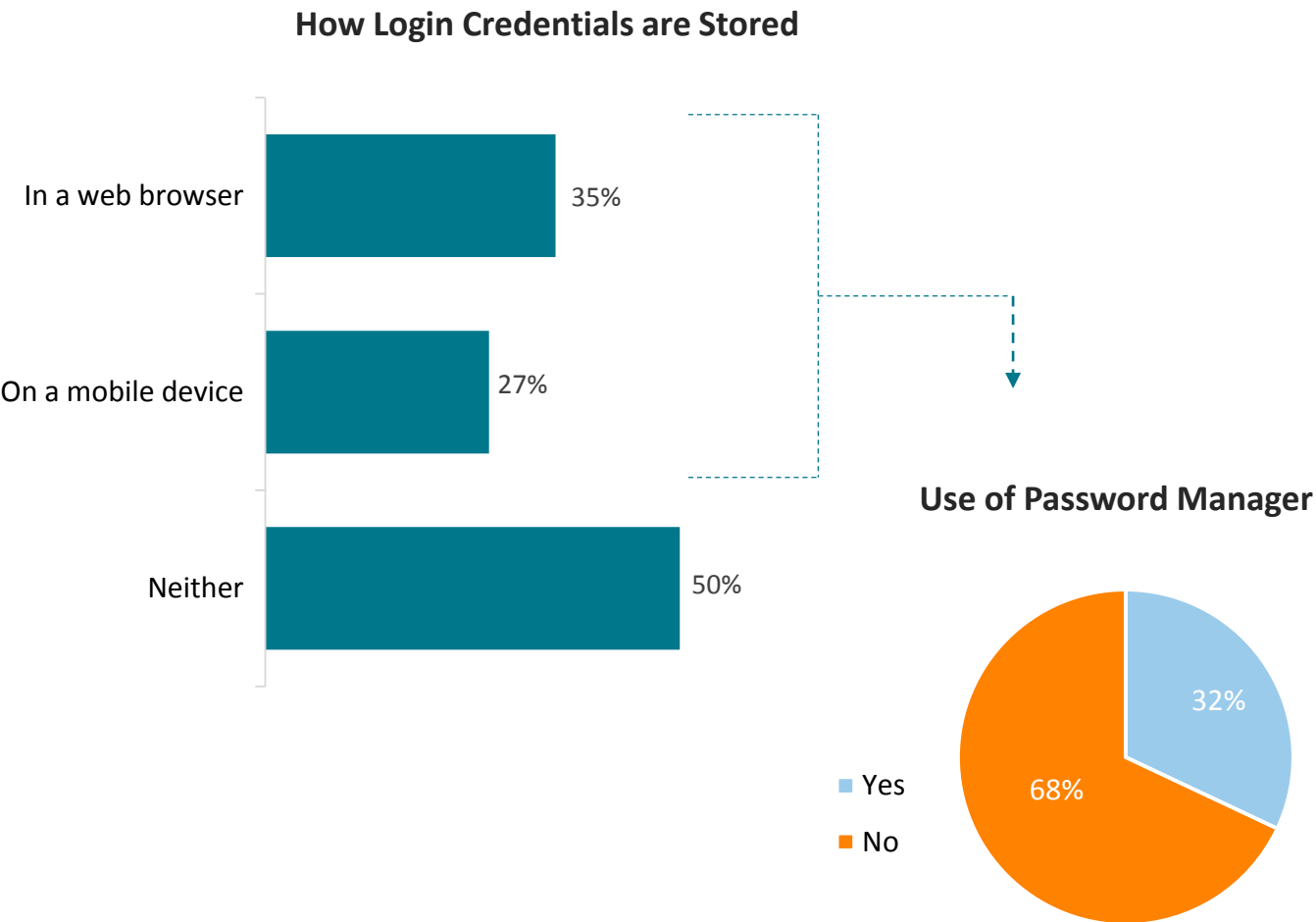


How much
customer friction
will Millennials
tolerate?



German Millennials are less likely to store credentials in a web browser, on a mobile device or in a password manager.

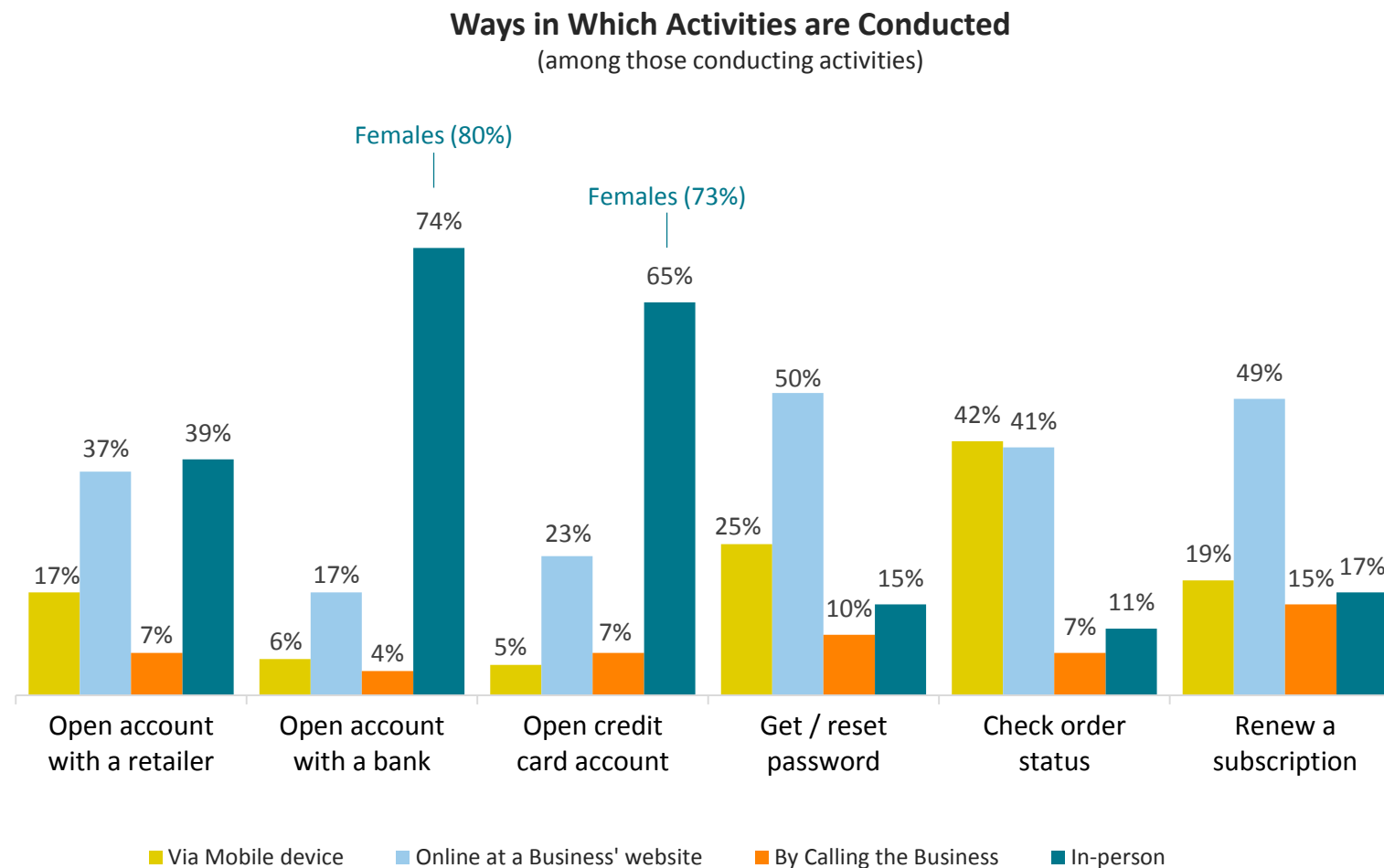
This supports the heightened sensitivity about access to one’s personally identifiable information.



Activities that involve higher risk, such as opening a bank account or new credit card, are more likely to be conducted in-person.

Lower risk, easy activities involving passwords, order status, and renewing subscriptions are most often done online. Female Millennials particularly prefer opening bank and credit card accounts in-person rather than through the anonymous online channel.

Millennials are mixed in terms of opening a retail account either in-person or online, likely depending on the degree of familiarity with the retailer (i.e., if more familiar, then more comfortable opening it online).



Not surprisingly, then, the preference to open new accounts in-person appears linked to concerns about security and control of one's personal information.

Over half of German Millennials (60%) who indicate that it is easier to open a new account in-person are likely saying this based on concerns about PII security; in reality, it's actually more convenient to open an account from the touch of a button than to physically travel to a provider's location.

German Millennials are particularly less confident about security of one's personal information in the mobile and Social Media channels.

Female Millennials are more likely than males to have these preferences and sensitivities.

Willingness to Provide Information for Services



Strongly Agree

- Prefer to open a new account in-person (61%; **Females 72% vs. Males 49%**)
- Easier to open a new account in-person (60%; **Females 68% vs. Males 52%**)
- Find it intrusive to provide financial information (55%; **Females 65% vs. Males 52%**)
- Cautious viewing banking info on a mobile device (51%)

Strongly Disagree

- Willing to access banking info via Social Media or mobile device (56%; **Females 62% vs. Males 49%**)

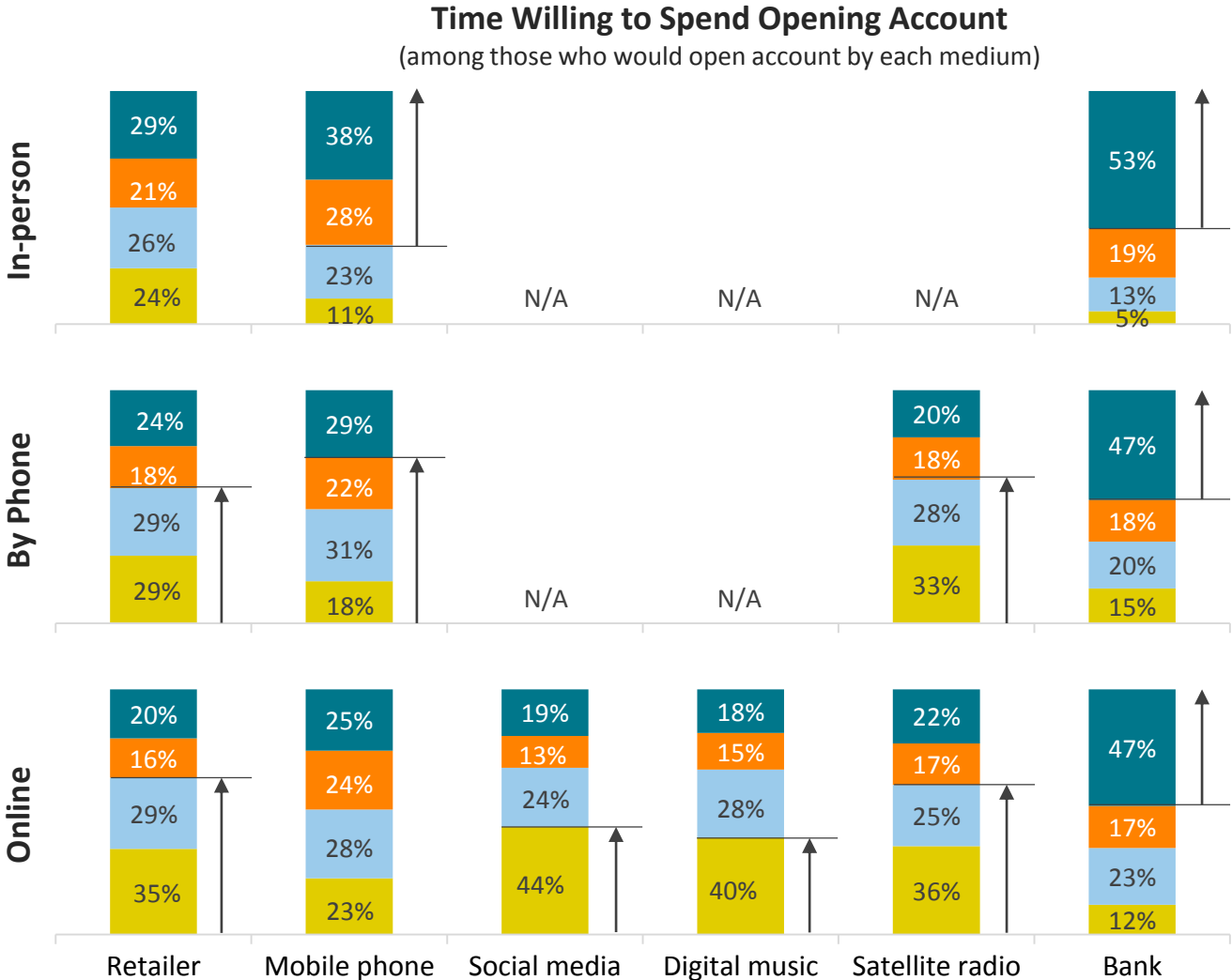
Therefore, German Millennials are willing to spend longer to open a bank account in-person than they are for other accounts via other channels.

A majority are willing to spend only 5-10 minutes opening a retail or satellite radio account, across mediums.

Millennials are willing to spend more time in-person than they are by phone or online when opening a mobile phone account.

Traditionally online accounts, such as social media and digital music, are expected to be opened in 5 minutes or less.

- < 5 minutes
- Up to 10 minutes
- Up to 15 minutes
- 30 minutes or more



Time is less of an issue during account opening than is the type and volume of information being requested.

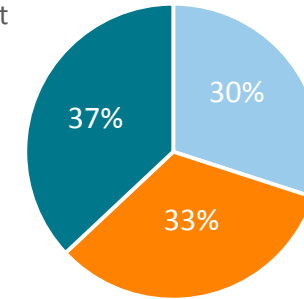
Millennials are mixed between willingness to provide more information when opening an account vs. accessing an existing one. Though, keeping in mind that they are uncomfortable providing personal information and much beyond two pieces on PII.

A majority are more likely to terminate an account opening session based on the type & amount information required (72%) than they are based on time (17%). This does not differ based on gender, even though Females are more concerned about information access and handling.

Females are, however, less likely than males to link to existing accounts in order to create a profile for new ones.

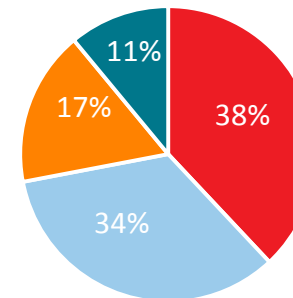
Willingness to Provide Information

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

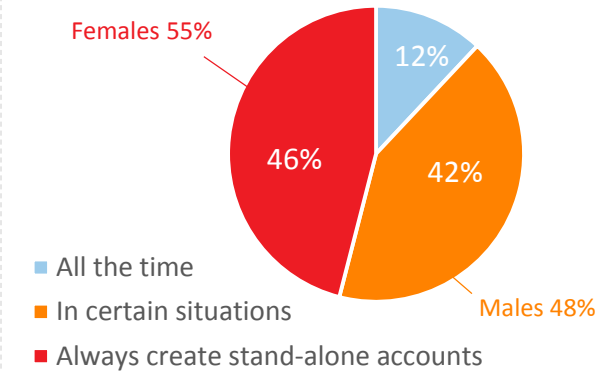


What Causes Termination of Account Opening Session?

- 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)



Conclusions



German Millennials are digitally connected and concerned about identity theft, yet there is apprehension about trusting companies with their personally identifiable information (PII) in order to protect it.

- On average, German Millennials use multiple devices, with over two-thirds conducting remote banking and purchasing.
- At the same time, they have concerns about the risk of online privacy (65%), too much collection of their PII by companies (63%), having their identity stolen through online / mobile / app-based activities (52%) and online protection through effective safeguards (only 17% feel protected).
 - Less than half (47%) feel that it is necessary for companies to even ask for their personal information in order to verify one's identity and prevent fraud.
 - Less than one-third fully trust financial institutions with handling their personal information; this drops considerably to less than one-fifth with regard to communications companies, payment providers and retailers.
 - Much of the above is even more pronounced among female Millennials.

German Millennials have mixed attitudes and behaviors towards identity protection and willingness to help companies protect them.

On one hand, they are consistent with . . .

Attitude	Behavior
Having concerns about their identity being compromised through data breaches and . . .	Being fiercely protective about giving their personal information to companies.
Having concerns about companies having too much of their personal information and . . .	Will terminate opening a new account if too much sensitive PII is asked.

On the other hand, they are inconsistent with . . .

Being worried about having their debit card information stolen, yet . . .	Use debit cards to make remote purchases directly with the provider.
Being worried about having their identity stolen through online/app-based/mobile activities, yet . . .	Use online and mobile browsing for purchases and financial transactions.
Not using mobile browser based devices (smartphones, tablets) for financial transactions, yet . . .	Some (56%) would be willing to access banking info via Social media and mobile devices.

Given that, German Millennials place limits on the amount friction they will accept to verify identity and prevent fraud.

- The more sensitive the information requested, the more concern that arises for them and the higher the likelihood that they will terminate at least a new / opening account.
- Motivating German Millennials to provide information in exchange for freebies may be tough.
 - Less than half (45%) would be willing to provide their shopping habits for this, with even fewer (32%) who would be willing to give their actual geographic location for targeted goods / services (and presumably unwanted ads and spam). This is consistent with their overly-protective mindset towards giving out PII.
- Control over one's PII and online/mobile data protection drives preferences when opening new accounts.
 - They prefer in-person rather than through anonymous channels and are willing to spend more time to do this for financial accounts.
 - While they will open new retail accounts online and have more limited time expectations (10–15 minutes) when doing so, keep in mind that the type of information requested is more of a deal-breaker than the amount of time spent opening a new account.
- Biometrics is being used to a degree. Trust is mixed among those who use it and very low among those who don't. However, few are comfortable allowing a company to gather information that enables biometrics for identity protection.
 - This suggests the need for more education about its ability to deliver enhanced security without requiring Millennials to give out more sensitive types of personally identifiable information.

All of this indicates that perceptions of control over one's PII is the key driver for the amount and type of information that German Millennials are willing to provide.

- The sizeable preference for opening accounts in-person supports this by eliminating the anonymous environment.
- German Millennials show some openness to new ways to doing things, such as linking new accounts to existing ones when establishing their profile – but, only for certain situations as they choose.
- Provider brand and familiarity can be a double-edged sword.
 - Familiarity / experience with the provider's brand likely influences the degree of information sharing.
 - However, the flip-side is the expectation that a provider already “knows me, so why ask for such sensitive data” unless it's fraudulent phishing.

Recommendations



For the skeptical German Millennials group, it will be important to limit the amount of PII that is requested of them for identity protection.

- Requests for too much or too sensitive information can be a deal-breaker for German Millennials. However, companies need to balance this friction with the need to protect themselves and their customers against fraud.
- To the degree available, pre-populated data could reduce this challenge.
- Enabling access to existing accounts through one-time passwords is not entirely unacceptable to German Millennials, though some still need further convincing. That said, this type of control lessens the bigger concern about having to give other / more sensitive data to companies (which is already a sore point among German Millennials).

Let LexisNexis® Risk Solutions tailor the authentication experience with a layered approach, such as One Time Password with Knowledge Based Authentication. This 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.

- It will be challenging for companies to gather much data from German 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).

The identity authentication process should be different based on the type of transaction experience (in-person, online, by phone).

- Since not all transactions have the same risk level (i.e., in-person versus mobile; high value items versus commodities), companies can minimize friction by adjusting the degree to which they ask for / use customer information across different transactions (i.e., pick their battles).
 - German Millennials approach transactions with an already heightened sensitivity to company use of their PII. Yet, at the same time, they also have concerns about fraudulent use of their debit cards and identity.
 - And, their stated level of patience and acceptable friction tends to differ by perceived risk. They are particularly more cautious about financial and mobile transactions.
 - Taken all together, this would suggest that there are times when they will accept more friction based on the higher value / perceived risk of the transaction – but not all the time. Therefore, the authentication process needs to have this flexibility to ensure the optimal customer experience.

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.



Appendix



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.