Digital Banking to replace bricks and mortar within 5 years
Gemalto’s eBanking Trends research revealed that nearly three quarters (72%) of IT and business decision makers from the banking sector predict that all customer interactions will be online in five years, despite them reporting that around two thirds (67%) of their customer base have the ability to use eBanking today.

The study, polling 900 IT and business decision makers from the banking sector and 11,000 consumers across 14 markets who use online/mobile banking, found that security remains a concern for both customers and decision makers. Over four in ten (44%) of customers cited that they would switch bank if their current bank had been breached, while two fifths (38%) would leave if they knew another provider was offering better security measures.

These concerns are clearly being noticed by decision makers, who believe that customer convenience (67%), customer demand (67%), keeping up with competitors (63%) and increasing security compared with traditional banking (54%) are the top reasons for them to invest in eBanking security solutions.

While banking leaders seem to be keen to invest in security, the traditional password continues to be the main security mechanism for eBanking solutions (81%), followed closely by transaction security (73%) and fraud management (64%). More sophisticated and secure protection methods are used less, with two-factor authentication (48%), encryption at rest (30%) and in transit (28%) and biometric solutions (28%) all further down the list.

For consumers, the main driver for using online and mobile banking is convenience (87%), with a further two-thirds (67%) believing that it is easier to use these solutions than visiting a branch. However, there are still concerns: half (51%) believe that there are security gaps in eBanking solutions, with a third (32%) thinking that using banking apps and websites put them and their personal information at risk. Perhaps more concerning for decision makers is that over half (54%) of consumers use the same password across multiple accounts.

To ensure that eBanking continues to evolve and begin to find a balance between security and convenience, decision makers are planning to improve their security features even further, with one-time passwords (48%) and two-factor authentication (48%) on top of the list, for those organisations that do not already offer these, in the next 12 months. Biometric security measures are also seen as key for the future, with fingerprint scanning (77%), face recognition (68%), voice recognition (66%) and iris recognition (61%) planned over the next five years.

Biometrics are also top of mind for consumers, with over half (55%) willing to use them for eBanking of which 80% believe that it is more secure than usernames and passwords, while two-fifths (41%) believe that they are more convenient than traditional methods.

Key areas of interest

Use of eBanking ........................................ 7
Drivers and benefits ................................. 10
Challenges and concerns .......................... 12
eBanking security ....................................... 14
The future of eBanking security .................. 22
### Key findings

<p>| 64% | Surveyed professional respondents estimate that 66% of their organization’s customer base have the ability to use eBanking, and out of these, 64% do use eBanking with them. |
| 67% | Predominately, banks are driven to implement eBanking solutions to answer customer demand (67%) and to improve convenience for the end users (67%). |
| 87% | Surveyed consumers use online and mobile banking because it is convenient (87%), with only 17% driven to use eBanking solutions because of the security it offers. |
| 56% | Despite this, 56% of surveyed professional respondents believe that their customers have seen greater security as a benefit of eBanking. |
| 44% | Nevertheless, 44% of surveyed consumers would still switch banks if their bank experienced a security breach. |</p>
<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>32%</td>
<td>For 32% of surveyed professionals, user negligence is only the second most common risk to the customer, despite 54% of consumers admitting they use the same password for multiple online accounts.</td>
</tr>
<tr>
<td>51%</td>
<td>Just over half of professional respondents believe that their organization’s customers are completely confident in their security mechanisms.</td>
</tr>
<tr>
<td>51%</td>
<td>The same percentage of surveyed consumers believe that there are gaps in eBanking security.</td>
</tr>
<tr>
<td>45%</td>
<td>Investments in biometric technologies are set to increase steadily over the next five years, with 45% of consumer respondents willing to use this, and 10% who already are.</td>
</tr>
<tr>
<td>72%</td>
<td>Almost three in four surveyed professional respondents agree that in five years’ time, all customer interactions with their services will be online.</td>
</tr>
</tbody>
</table>
Use of eBanking

How many are using eBanking?
Surveyed professional respondents estimate that just over two thirds (66.52%) of their organization’s customers have the ability to use eBanking solutions (fig. 1). Out of these, 64% are estimated to be using eBanking services with surveyed respondents’ banks (fig. 2).

Figure 1
“What percentage of your organization’s customer base do you estimate have the ability to use eBanking (either online or on a mobile app)”

Figure 2
“What percentage of your organization’s customer base who have the ability to use eBanking, actually use it?”
What type of eBanking is in use?
According to surveyed professionals, online banking is incontestably the most used eBanking solution. 96% of them estimate that their customers use online banking services. The mobile channel is not far behind as 79% estimate that their customers also use their banking app.

These high percentages demonstrate that many customers will be using both types of eBanking. 23% of them report using mobile banking services on a daily basis. And 29% connect to their online banking every couple of days. On average, they log in their online banking 4 times a week (fig. 4).

On average, consumers log in to their online/mobile banking 4 times a week.

Figure 3
"Which of the following eBanking solutions do your customers use with your organization?"

- Online banking: 96%
- Mobile app: 79%

Figure 4
"How frequently do you log onto the following?”, asked to all 1,150 respondents, only seeing the eBanking types in use [base in chart].

- Mobile banking:
  - Several times a day: 9%
  - Daily: 23%
  - Every couple of days: 28%
  - Weekly: 24%
  - Monthly: 13%
  - Less frequently: 3%

- Online banking:
  - Several times a day: 7%
  - Daily: 20%
  - Every couple of days: 29%
  - Weekly: 28%
  - Monthly: 14%
  - Less frequently: 2%

Asked to all 900 professional respondents.
Most popular eBanking services

With so many consumers reporting to frequently connect to their online and mobile banking accounts, it is not a surprise to see that the most popular use cases are checking balances (81%) and internal transfers between personal accounts (71%) (fig. 5).

It seems that online and mobile banking services have replaced the physical branch for simple daily operations. However, it is likely that consumers are still reluctant to execute more complex and sensitive operations online. Indeed, according to banks, only 23% of their customers apply for a loan online or using their banking mobile app.

Checking balances is the consumers’ favorite use case for online and mobile banking according to 81% of banks.

Figure 5

“Which of the following services are most commonly used online/on a mobile app by your organization’s customer base? Combination of responses ranked first, second and third”

<table>
<thead>
<tr>
<th>Service</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checking balances</td>
<td>81%</td>
</tr>
<tr>
<td>Internal transfers</td>
<td>71%</td>
</tr>
<tr>
<td>External transfers</td>
<td>53%</td>
</tr>
<tr>
<td>Setting up direct debits/standing orders</td>
<td>36%</td>
</tr>
<tr>
<td>Loan applications</td>
<td>23%</td>
</tr>
<tr>
<td>Updating profiles</td>
<td>20%</td>
</tr>
<tr>
<td>Searching for help and support</td>
<td>16%</td>
</tr>
</tbody>
</table>
Drivers and benefits

Consumers’ drivers to use eBanking services
The results of our survey clearly show that convenience is the key driver for consumers to use eBanking. 87% say that they use online and/or mobile banking services because it is convenient. 67% add that it is a good alternative to in-branch banking (fig. 6). These results corroborate the findings described in figure 5. Consumers want simplicity and convenience for their daily operations and are most likely to visit a physical branch for more complex operations. Indeed, only 16% say that the branch is dying out.

Security does not seem to be a significant driver for digital banking. It is the third reason named by consumers to use online/mobile banking, after convenience and innovation. Only 17% say that they choose to bank online or on their mobile devices because they consider it more secure.

87% of consumers use eBanking services because it is convenient.

Banks’ drivers to invest in eBanking security solutions
The banks’ drivers to invest in eBanking solutions seem to be in line with consumers’ feedbacks. 67% say that they invest to provide more convenience to end users, and another 67% say their investments are driven by customer demands (fig. 7).

It looks like banks are well aware of their customers’ needs and expectations and adapt their investments accordingly. With the increasing success of online and mobile banking, it is encouraging to see that 54% of banks invest to increase security.

What benefits does eBanking offer the bank and the customer?

Figure 6
“What are the reasons why you use online/mobile banking?”

- It is convenient 87%
- It is easier than going into branch/in-store 67%
- Online/mobile banking is more innovative 22%
- It is more secure to bank this way 17%
- Branch/in-store banking is dying out 16%
- My bank is an online/mobile only service 14%
- I get better incentives banking this way 11%
- I get better overall rates banking this way 10%
- Other 11%

Asked to all 900 professional respondents

Figure 7
“What were your organization’s main drivers for investing in eBanking security solutions? Combination of responses ranked first, second and third”

- Convenience for customers 67%
- Responding to customer demand 67%
- Keeping up with competition 63%
- Increase security 54%
- Regulation 26%
- To be cost-effective 24%

Asked to all 900 professional respondents
Business and customer-focused benefits

99% of banks report that their organization has seen benefits since implementing eBanking solutions, including 78% who have seen customer loyalty increase, and 70% who have seen greater internal operational efficiency (fig. 8).

Similarly, all professional respondents believe eBanking has resulted in benefits to the customer, including increased satisfaction (72%) and more convenience (65%) (fig. 9).

According to these respondents, both the organization and customer has benefited from greater security (55% and 56% respectively – fig. 8 and 9), despite only 17% of customers who report better security to be a driver to using eBanking (fig. 7).

**Figure 8**
“Which of the following benefits have been seen in your organization as a result of implementing eBanking solutions?”

- Increased customer loyalty: 78%
- Greater operational efficiency: 70%
- Competitive advantage: 65%
- Greater security of customer data: 55%
- Assured compliance: 31%
- My organization has not seen any business benefits: 11%

**Figure 9**
“Which of the following benefits have your customers experienced as a result of your organization offering eBanking solutions?”

- Increased satisfaction: 72%
- More convenience: 65%
- Improved customer experience: 60%
- Greater security: 56%
- Greater simplicity compared to other banking methods: 47%
- Better rates: 35%
- Better offers: 32%
- Greater innovation: 30%
Implementation challenges
Implementing eBanking services is a challenging project for banks. 60% of the professional respondents find that the main difficulty is to build customer trust in new solutions (fig. 10). Banks have to make a lot of education efforts in order to boost customer adoption.

Security is also a key concern for banks with more than half of them saying that security is one of their main challenges when implementing eBanking solutions.

96% of surveyed professional respondents report that their organization has faced challenges when implementing eBanking solutions.

Figure 10
"Which of the following challenges has your organization faced when implementing eBanking solutions for your customers?"

What do banks look for when finding a trusted partner to work with?

Asked to all 900 professional respondents

- Build customer trust in new solutions: 60%
- Concerns around security: 55%
- Find a trusted partner to work with: 45%
- High competition: 42%
- Lack of/ poor infrastructure: 28%
- Lack of board support: 20%
- Lack of in-house skills: 16%
- My organization has not faced any challenges when implementing eBanking solutions: 6%
Reasons why consumers would switch banks

Despite only 17% of consumers reporting security as a key driver to use online and mobile banking, 38% of them say that they would switch banks if they were offered better security elsewhere. A security breach would also be a deal breaker for 44% of them (fig. 12). Consumers are mostly driven to use eBanking because they find it convenient, they also want strong security and are not ready to make any trade off between convenience and security. They want both and it is up to the banks to find the right balance.

The consumer’s perception of security is likely more of a factor than banks realise, so it is positive that they already use security as a driver for implementing eBanking solutions (fig. 6) and that they want to work with technology partners who are strong in this area (fig. 11).

In case of a security breach, 44% of consumers would switch banks.

Must-haves when working with a technology provider

Generally, surveyed professional respondents are seemingly picky when choosing a trusted technology partner to work with, with all options cited as being ‘a critical must-have factor’ by at least a third or more.

The most common must-have factor is them having strong security solutions in place (71%), followed by security certification (70%), echoing the second most common challenge banks face when implementing eBanking solutions (fig. 10).

One of the least ‘critical’ factors is low cost/value for money (43%), demonstrating that organizations are willing to pay for good quality solutions and support.

---

**Figure 11**

“What of the following factors are critical when it comes to choosing a trusted technology or security partner to work with?”

- Strong security solutions: 71%
- Security certification: 70%
- Compliance with main regulations: 63%
- Reputation: 60%
- Industry expertise: 54%
- Ability to provide a complete offering: 53%
- Resilience/market staying power of the company: 49%
- Low cost / good value for money: 43%
- Bespoke service: 38%

---

**Figure 12**

“What factors would/do cause you to switch bank?”

- If my bank experienced a security breach: 44%
- Better overall rates on offer: 41%
- Better security from other banks: 38%
- Received incentives to switch from other banks: 27%
- Want to bank with a bank that is known for customer service: 21%
- Want a bank that is known for innovation: 14%
- Negative media attention: 13%
- Other: 18%

---

**Figure 12**

“Which of the following factors are critical when it comes to choosing a trusted technology or security partner to work with?”

- Strong security solutions: 71%
- Security certification: 70%
- Compliance with main regulations: 63%
- Reputation: 60%
- Industry expertise: 54%
- Ability to provide a complete offering: 53%
- Resilience/market staying power of the company: 49%
- Low cost / good value for money: 43%
- Bespoke service: 38%

**Figure 11**

“Which of the following factors are critical when it comes to choosing a trusted technology or security partner to work with?”

- Strong security solutions: 71%
- Security certification: 70%
- Compliance with main regulations: 63%
- Reputation: 60%
- Industry expertise: 54%
- Ability to provide a complete offering: 53%
- Resilience/market staying power of the company: 49%
- Low cost / good value for money: 43%
- Bespoke service: 38%
eBanking security

Risks to security
Even though consumers seem to be preoccupied with security (fig. 12), a majority of them have risky behaviors online. Over half (54%) of surveyed consumers say that they use the same password across accounts (fig. 13).

Despite this, surveyed professional respondents only cite user negligence (32%) as the second most common risk to customers using eBanking, with hackers targeting databases being the most common risk (36%) (fig. 14).

This suggests that not only are there more worrying risks to deal with (such as ransomware attacks and data breaches etc.), but that banks are perhaps not putting as much emphasis on protecting the user from themselves. Indeed, while two thirds (67%) of banks are concerned by data breaches in the transaction process, only 52% are concerned with user error (fig. 15), highlighting the lower emphasis placed on consumer behavior.

It is encouraging to see that almost all banks (99%) are looking to counteract these security concerns, most commonly by partnering with the right security solution provider (69%) and by improving customer education around eBanking security (65%) (fig. 16).

**Figure 13**
“Do you tend to use the same password across all your accounts? (online banking and social media accounts)”

- Yes, for all of my accounts: 46%
- Yes, for some of my accounts: 13%
- No, I do not use the same password for any of my accounts: 40%

**Figure 14**
“What do you perceive to be the biggest risk consumers using eBanking solutions?”

- Hackers targeting databases storing financial data/information: 36%
- User negligence: 32%
- Poor security measures: 17%
- Malicious insider activity (e.g., employees acting fraudulently): 8%
- Foreign government hacks: 3%
- I do not belief consumers are at any risk: 5%

 Asked to all 11,000 consumer respondents

 Asked to all 900 professional respondents
Figure 15

“What are the main concerns around security that come from supporting eBanking solutions in your organization?”

- Data breaches in the transactional process: 67%
- Fraud liability: 65%
- Data breaches on internal systems (resulting in loss of user/financial information): 57%
- User error: 52%
- Regulation/compliance breaches: 33%
- We do not have any concerns around eBanking security: 2%

As asked to all 900 professional respondents.

Figure 16

“In what ways is your organization addressing or planning to address security concerns from supporting eBanking solutions?”

- Partnering with the right security solutions provider: 69%
- Customer education around eBanking security: 65%
- Regular audits to ensure adherence to regulations: 55%
- Real time fraud detection and prevention: 49%
- Getting consultancy: 48%
- We have thought about/decided how we will address these concerns: 1%

As asked to 880 professional respondents whose organization has at least one concern around eBanking security.
Security mechanisms in place – the banks’ perspective

It seems that banks have implemented a wide range of security measures in order to protect their eBanking services, spanning from simple password (81%) to fraud and risk management (64% and 52%) (fig. 17).

Banks understand that a multi-layered approach is necessary when it comes to securing their customers’ sensitive data.

Consumers are aware of the eBanking security measures put in place by their banks, with even 30% of them who know that their bank use encryption (fig. 18).

**Figure 17**

"Which of the following security methods are in place in your organization’s eBanking solutions?"

- **Passwords**: 81%
- **Transaction security**: 73%
- **Fraud management**: 64%
- **Risk management**: 52%
- **Two-factor authentication**: 48%
- **Encryption (data at rest)**: 30%
- **Encryption (data in transit)**: 28%
- **Biometrics**: 28%

Asked to all 900 professional respondents
Consumers’ opinion mirror the mechanisms that the professionals report to be in place (fig. 17), suggesting that lines of communication around security are open between the bank and the consumer.

**Figure 18**
"Which of the following security measures are in place for your online banking?"

- Passwords: 84%
- Transaction security: 50%
- Two-factor authentication: 43%
- Encryption: 30%
- Fraud and Risk management: 23%
- Biometrics: 13%
- Other: 1%
- Don’t know: 5%

Asked to 10,392 consumer respondents who use online banking

**Figure 19**
"Which of the following types of security are in place for your mobile banking?"

- Passwords: 82%
- Transaction security: 47%
- Two-factor authentication: 41%
- Encryption: 27%
- Fraud and Risk management: 24%
- Biometrics: 17%
- Other: 1%
- Don’t know: 5%

Asked to 6,476 consumer respondents who use mobile banking
**Professional perception of consumer confidence**

Only 5% believe their customers have no confidence in their security measures.

Generally, banks are very confident when it comes to how their security is perceived among end users, which is positive considering so many (44%) consumers would switch banks if a breach occurred (fig. 12).

<table>
<thead>
<tr>
<th>Perception of Security</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completely confident</td>
<td>51%</td>
</tr>
<tr>
<td>Somewhat confident</td>
<td>40%</td>
</tr>
<tr>
<td>No confidence</td>
<td>5%</td>
</tr>
<tr>
<td>No opinion</td>
<td>3%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>2%</td>
</tr>
</tbody>
</table>

*Figure 20*

“Do you believe that your customers are confident in your organization’s mobile and online banking security mechanisms?”

As asked to all 980 professional respondents.
Consumer perception of eBanking security

Even though consumers are mainly using eBanking because it is convenient, they are also concerned about security. Just over half (51%) of surveyed consumers believe that there are gaps in the security of online and/or mobile banking (fig. 21).

Additionally, around a third (32%) consider that banking apps and websites expose them and their personal information to risk (fig. 22).

Perhaps the confidence that banks put into their security, and therefore the perception they have of their consumers’ trust (fig. 20) is slightly misguided, and businesses should not rest easy assuming their customers are happy and feel safe.

**Figure 21**
“In your opinion, is online/mobile banking secure?”

- Yes, completely: 4%
- No, there are some gaps in security: 39%
- No, there are major gaps in security: 47%
- Don’t know: 10%

As asked to all 11,000 consumer respondents.

**Figure 22**
“Which apps/websites do you feel expose you and your personal information to the greatest risk?”

- Social media: 62%
- Torrent sites: 39%
- Adult content sites: 38%
- News and information services: 29%
- Online streaming services: 23%
- Website search services: 21%
- Travel companies: 11%
- Bank: 32%
- Other apps/websites: 1%
- There are not any apps/websites that pose the greatest risk: 9%

As asked to all 900 professional respondents.
Security solutions in the future

The most common security solutions that banks plan to offer in the next twelve months are one-time passwords (48%) and two-factor authentication (48%).

eCommerce security solutions are also considered by banks, as 30% of them are looking at implementing 3D Secure systems in the next 12 months and 32% plan to deploy Dynamic CVV (fig. 23).

Banks have definitely their eyes on biometric authentication, with 34% of them planning to implement fingerprint solutions in the next 12 months, and 24% planning to implement face recognition in the next 24 months (fig. 23).

Figure 23

"Which of the following security solutions does your organization plan to implement in the following timeframes?"

<table>
<thead>
<tr>
<th>Security Solution</th>
<th>In the next 12 months</th>
<th>In the next 24 months</th>
<th>Beyond 5 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>One time passwords</td>
<td>48%</td>
<td>19%</td>
<td>9%</td>
</tr>
<tr>
<td>Two-factor authentication</td>
<td>48%</td>
<td>24%</td>
<td>11%</td>
</tr>
<tr>
<td>3D secure for eCommerce</td>
<td>30%</td>
<td>28%</td>
<td>17%</td>
</tr>
<tr>
<td>Dynamic CVV</td>
<td>32%</td>
<td>27%</td>
<td>17%</td>
</tr>
<tr>
<td>Fingerprint scanning</td>
<td>34%</td>
<td>26%</td>
<td>17%</td>
</tr>
<tr>
<td>Face recognition</td>
<td>22%</td>
<td>24%</td>
<td>22%</td>
</tr>
<tr>
<td>Voice recognition</td>
<td>23%</td>
<td>24%</td>
<td>20%</td>
</tr>
<tr>
<td>Iris recognition</td>
<td>18%</td>
<td>22%</td>
<td>21%</td>
</tr>
</tbody>
</table>

As asked to all 900 professional respondents
Biometrics – why?
Consumers are eager to use biometrics for mobile banking. Even though only 10% of surveyed consumers currently use biometric technology for mobile banking, an additional 45% would be willing to if their bank offered it.

Interestingly enough, the main reason why consumers are willing to use biometrics is not convenience but perception of security. 80% of them say that biometric authentication seem more secure than the traditional username/password. End users feel safer and more confident using biometrics for mobile banking.

The investment in biometrics planned by banks across the next five years (fig. 26) is well-placed, considering many consumers are ready to use it.

Figure 24
“Are you willing to use biometric security measures for mobile banking?”

Figure 25
“Why are you willing to use biometric security measures?”

- It seems more secure than a username / password
- It is convenient
- It saves time
- It is trendy
- Other

Asked to all 11,000 consumer respondents

Asked to 6,028 consumer respondents who are willing to use biometric security measures
Biometrics – which types?
Without any surprise, fingerprint is the most popular biometric method consumers are ready to use for authentication. A third would use voice recognition, and over two fifths would use face (42%) and iris (46%) recognition.

5% would even consider using their own blood to log into their accounts securely.

These results reveal that consumers are open to new authentication methods as long as it feels secure and convenient.

Predicted future for online banking
This prediction means big changes for banks, as traditional in-branch banking becomes a thing of the past.

In the future, banks will need to make greater investments in security than ever before, as customers will not have any other option to turn to, should online banking fail them.

Almost three quarters (72%) of surveyed professional respondents agree that in five years’ time, all customer interaction with their businesses will be online.

Figure 26
“What type of biometric security measures are you willing to use?”

- Fingerprint: 86%
- Iris recognition: 46%
- Face recognition: 42%
- Voice recognition: 34%
- Blood sample: 5%

Asked to 6,028 consumer respondents who are willing to use biometric security measures.

Figure 27
“To what extent do you agree with the following statement? : In five years’ time, all customer interactions with my business will be online.”

- Completely agree: 36%
- Slightly agree: 15%
- Neither agree nor disagree: 11%
- Slightly disagree: 3%
- Completely disagree: 3%

Asked to all 900 professional respondents.
In Summary

The introduction of online and mobile banking have given customers a convenient way to interact with their bank as and when they please. However, with so many consumers still feeling that there are gaps in eBanking security, it’s clear that banks need to optimize security without compromising on convenience before these digital services can achieve their full potential. Without this, banks risk losing consumer trust, with many taking their business elsewhere. The static PIN/password is no longer a secure enough solution. Banks understand that strong two-factor authentication combined with additional security layers such as risk management and encryption, is a must.

More and more financial institutions are now looking into biometrics to replace the PIN/password and increase convenience for daily banking operations. It’s great to see that banks are taking notice of customer demands for both stronger security and better user experience. Technologies such as fingerprint and facial recognition, which are widely acclaimed by consumers, allow banks to embrace their digital transformation and bolster security while improving convenience.
Demographics - professionals

900 IT and business decision makers from the banking sector were interviewed in October and November 2016, split in the following ways.

### Country

<table>
<thead>
<tr>
<th>Country</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>200</td>
</tr>
<tr>
<td>UK</td>
<td>100</td>
</tr>
<tr>
<td>Germany</td>
<td>100</td>
</tr>
<tr>
<td>Sweden</td>
<td>90</td>
</tr>
<tr>
<td>France</td>
<td>100</td>
</tr>
<tr>
<td>UAE</td>
<td>50</td>
</tr>
<tr>
<td>South Africa</td>
<td>500</td>
</tr>
<tr>
<td>Japan</td>
<td>50</td>
</tr>
<tr>
<td>Australia</td>
<td>80</td>
</tr>
<tr>
<td>India</td>
<td>100</td>
</tr>
<tr>
<td>Brazil</td>
<td>50</td>
</tr>
</tbody>
</table>

### Function

<table>
<thead>
<tr>
<th>Function</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business/development/sales/channel</td>
<td>387</td>
</tr>
<tr>
<td>IT</td>
<td>171</td>
</tr>
<tr>
<td>Product marketing</td>
<td>342</td>
</tr>
</tbody>
</table>

### Bank type

<table>
<thead>
<tr>
<th>Bank type</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regional retail bank</td>
<td>286</td>
</tr>
<tr>
<td>Global retail bank</td>
<td>176</td>
</tr>
<tr>
<td>Regional commercial bank</td>
<td>158</td>
</tr>
<tr>
<td>Global commercial bank</td>
<td>156</td>
</tr>
<tr>
<td>Investment bank</td>
<td>76</td>
</tr>
<tr>
<td>Central bank</td>
<td>33</td>
</tr>
<tr>
<td>Savings, loans and or mortgages only</td>
<td>15</td>
</tr>
</tbody>
</table>
Demographics - consumers

11,000 consumers who use online/mobile banking were interviewed in October and November 2016, split in the following ways.

**Gender**

- Male: 5528
- Female: 5456
- Prefer not to say: 16

**Age**

- 18-24 years old: 1878
- 25-34 years old: 2008
- 35-44 years old: 1953
- 45-54 years old: 1907
- 55-64 years old: 1834
- >65 years old: 1398
- Prefer not to say: 22
ABOUT GEMALTO

Gemalto (Euronext NL0000400653 GTO) is the global leader in digital security, with 2015 annual revenues of €3.1 billion and customers in over 180 countries. We bring trust to an increasingly connected world.

Our technologies and services enable businesses and governments to authenticate identities and protect data so they stay safe and enable services in personal devices, connected objects, the cloud and in between. Gemalto’s solutions are at the heart of modern life, from payment to enterprise security and the internet of things. We authenticate people, transactions and objects, encrypt data and create value for software – enabling our clients to deliver secure digital services for billions of individuals and things.

Our 14,000+ employees operate out of 118 offices, 45 personalization and data centers, and 27 research and software development centers located in 49 countries.

For more information visit:
www.gemalto.com/ebanking
www.gemalto.com/ebanking-security