



The State of

# Secure Digital Banking in US Retail Banks 2020



# Table of Contents

Executive Summary	3
Introduction: Challenges and Opportunities for Secure Digital Banking	4
Part 1: Customers Are Eager For Digital Banking	6
Part 2: Digital Banking Still Perceived As Less Secure Than In-Person	8
Part 3: Key Issues in Digital Banking	9
Security Issues Are An Obstacle For Seniors to Go Digital	9
Safe Digital Banking Is Paramount For High-Value Customers	12
Part 4: Cumbersome Digital Security is Costing Banks Heavily	15
Part 5: More Seamless Security Requirements Needed	19
Conclusion: Investing in Customers' Peace of Mind and Ease of Use	21

# Executive Summary

Prompted by consumer demand and the coronavirus, banks are increasing their investment in digital banking options like never before. But lingering security concerns are holding customers back from using digital services for all their financial needs. This is especially true for senior citizens and higher-income customers who have lingering security concerns.

At the same time, banks must be sure that the security measures they adopt don't add friction and actually help foster the streamlined, effortless, and efficient experience expected from the online sphere. Fortunately, there are many solutions on the market today that allow security and convenience to coexist, increasing the ROI banks receive from their investment in a digital transformation.



# Introduction: Challenges and Opportunities for Secure Digital Banking

Customers are showing unprecedented interest in digital banking in light of coronavirus-accelerated digital and remote trends. To better serve customers and benefit from more cost-effective processes, banks are beginning to view digital channels not as nice-to-have alternatives, but essential to their core operations.

Yet customers and bankers alike continue to depend on in-branch services, especially for more complex or financially significant activities. We suspected that security and privacy concerns were at the root of this hesitation to leap to fully digital banking, and wanted to find out if this was correct.

To that end, Lightico surveyed 1,329 Americans in July 2020 to assess their levels of trust in their banks' digital banking offerings. We found that despite the widespread usage of digital channels during the coronavirus era, many consumers continue to view in-person banking as the most secure channel.

Banks that want to accelerate uptake of a wider variety of digital banking transactions will need to implement security features that reduce consumer fear and confusion. This is particularly urgent for higher-income customers, who view their finances as more sensitive, and older customers, who still don't fully trust digital banking.

At the same time, it's not just more security that's needed, but seamless security; bulky and complex security measures defeat the purpose of digital banking, which is to provide efficient and fast customer experiences.



Fortunately, many cutting-edge solutions have emerged specifically to address this tension between security and efficiency. Some of these solutions provide easier and more effective ways for customers to access their bank accounts. Others are designed to facilitate secure transactions at different stages of the customer journey. By adopting such technologies, banks will be better equipped to capture new business opportunities and maintaining existing ones via digital channels.

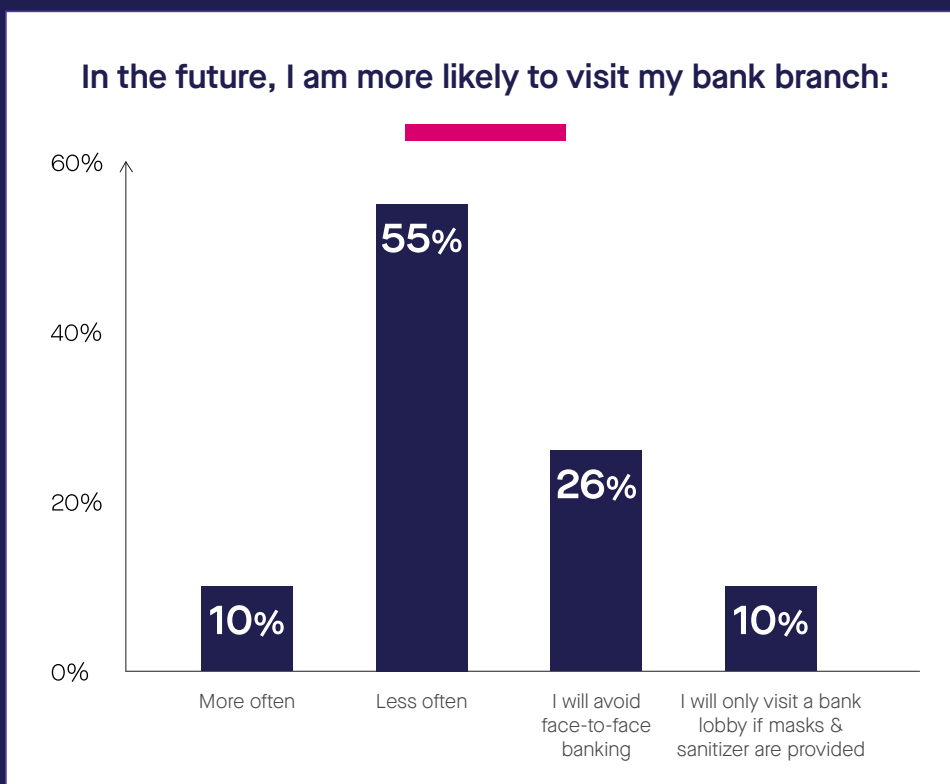


## Part 1

# Customers Are Eager For Digital Banking

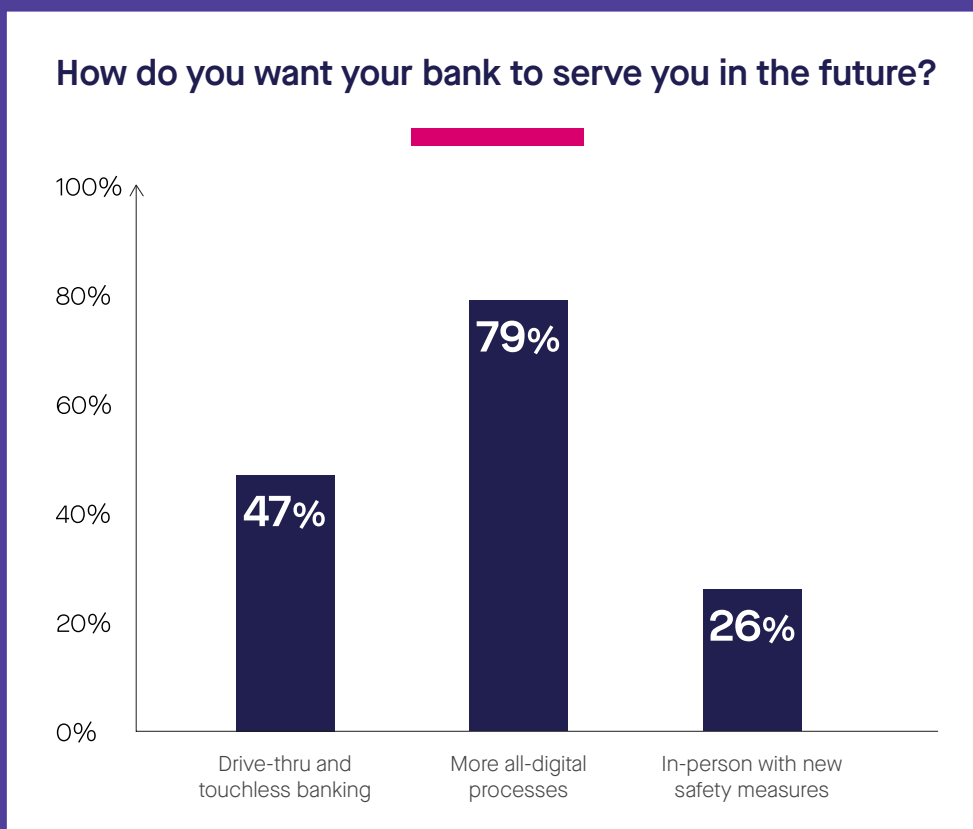
Consumers have plenty of opportunities in their daily lives to engage in different online transactions. From ordering groceries to filing for insurance to booking appointments at government offices, completing activities online has never been so simple or so prevalent. This is especially true in light of the coronavirus, which has led institutions, companies, and customers to see digital service as an essential service.

The coronavirus has all but made in-person banking a last resort for both customers and banks alike. Many banks have invested significant resources in transitioning to remote banking, and are heavily advertising those options. Most obviously, the purpose of doing so is to safeguard the health of agents and customers, who continue to fear virus transmission even as official coronavirus restrictions are lifted across the country.



At the same time, customers are in no rush to return to the physical branch, even once the threat of the virus fades away. 55% of customers say that they will visit their bank less often in the future, and 26% say they will try to avoid in-person banking altogether. These dramatic findings suggest that the coronavirus lockdowns enabled customers to gain unprecedented comfort with digital banking.

In fact, an unbelievable 79% of respondents say they want their banks to serve them with “more all-digital processes” going forward.

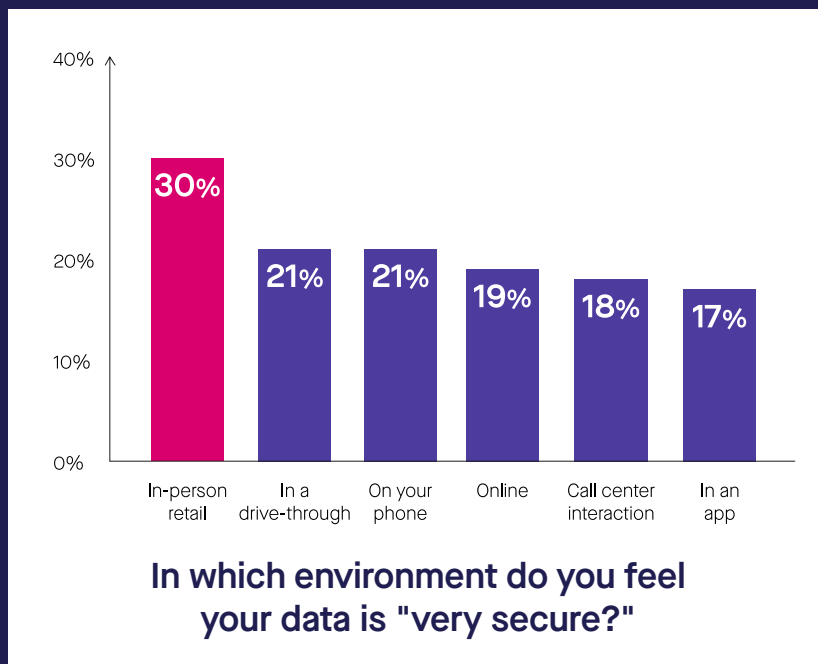


It makes sense: Why should customers drag themselves to a physical branch, which requires them to be in a particular place within a limited time frame, when they can receive instant service from the comfort of their computer or mobile phone?

**79% of banking customers want more all-digital banking processes, even after the coronavirus crisis ends.**

## Part 2

# Digital Banking Still Perceived As Less Secure Than In-Person



Despite high levels of interest in digital banking, consumers are torn: On the one hand, they would love to rely on remote banking transactions thanks to the significant convenience advantages. On the other hand, in-person banking is still widely seen as the most secure choice.

30% of consumers say they fully trust the security of their data during in-person transactions at a bank, compared to just 19% who say the same about online transactions.

What this disparity suggests is that customers may be very open to and even prefer using digital tools for simple tasks, such as checking their bank balance or requesting a new credit card. But when it comes to more involved tasks, such as transferring large sums of money or taking out a loan, they may still choose in-person banking due to the greater perception of security.

Our survey found that two groups in particular — senior citizens and higher-income earners — are very interested in digital banking but their needs for seamless security remain unmet. These groups' concerns must be addressed if banks want to attract and retain them as customers. We will discuss these unique populations in the following sections.



## Part 3

# Key Issues in Digital Banking

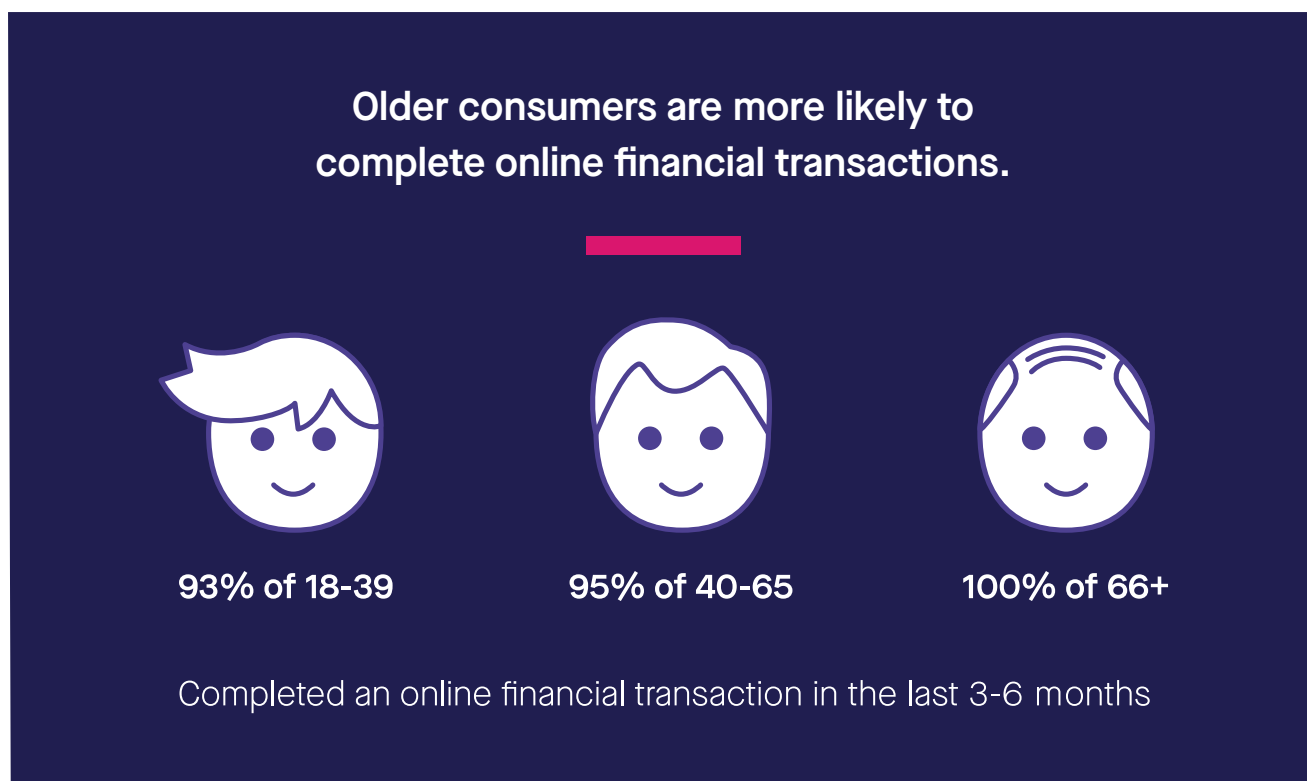


## Security Issues Are An Obstacle For Seniors to Go Digital

There's a common stereotype of older people as technophobes—eschewing the conveniences of technology in favor of pen-and-paper or face-to-face interactions. Yet the research shows that this is no longer the case. The coronavirus pandemic has only accelerated growing digital and remote trends, forcing unlikely groups, including older people, to interact with technology like never before.



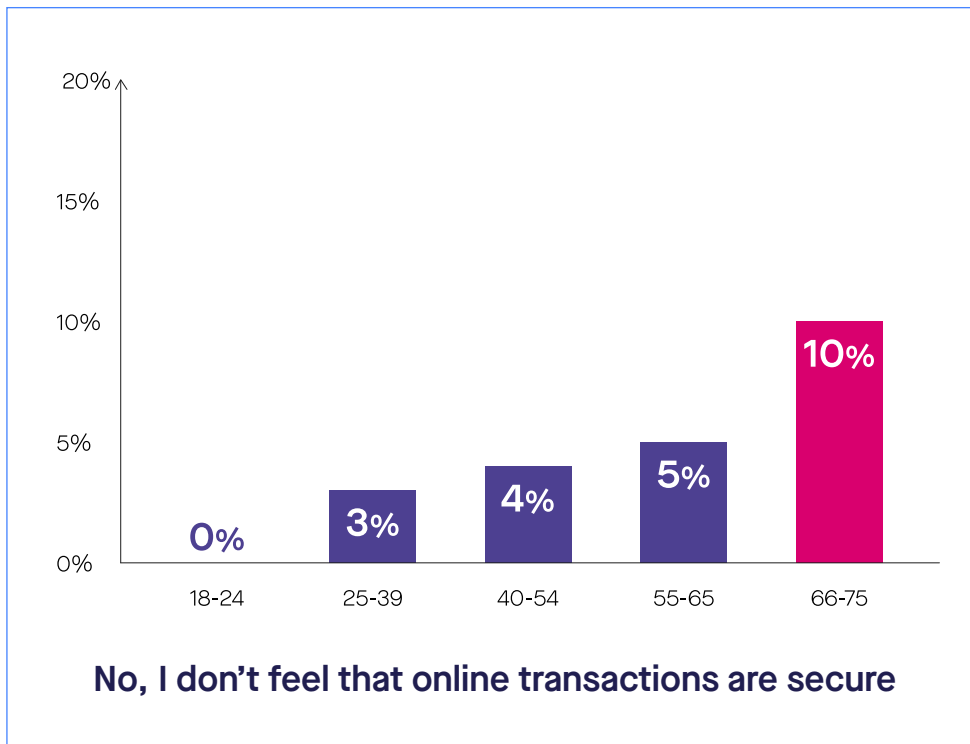
## A Digital Divide Over 65? Don't Be So Fast to Assume.



Compared to their younger counterparts, older people are even warier of in-branch banking due to the increased health risk posed by the coronavirus. The results were dramatic: 100% of the older consumers (aged 66-75) we surveyed say they have completed an online financial interaction in the last three to six months. In contrast, a smaller but still very large proportion (93%) of 18 to 39-year-olds have done so.

Health factors aside, it's highly likely that senior citizens have also gained unprecedented comfort with digital banking due to the necessity of establishing new remote habits. By the time the coronavirus crisis is over, seniors will have become so accustomed to taking care of their finances online that going to a physical branch will seem like an unnecessary hassle.

## Yet Banking Security Remains a Concern For Seniors



Despite record-high use of digital banking among senior citizens, lingering fears about online security lurk under their surface acceptance of digital tools. 10% of senior citizen bankers don't feel online transactions are secure (even larger proportions see them as merely “somewhat secure” — also not a rousing endorsement).

When asked to rank their top concerns regarding online security, the majority fear financial loss first (52%), and loss of privacy second (42%). Seniors, who are often on fixed incomes and may already feel financially vulnerable, are especially worried about the potential monetary loss from online identity theft.

It may be that seniors are currently using digital bank tools for the most rudimentary of tasks, such as checking their bank balance. But if seniors are avoiding opening a new account, transferring money, or other more complex tasks due to security concerns, this represents lost opportunities for the bank.



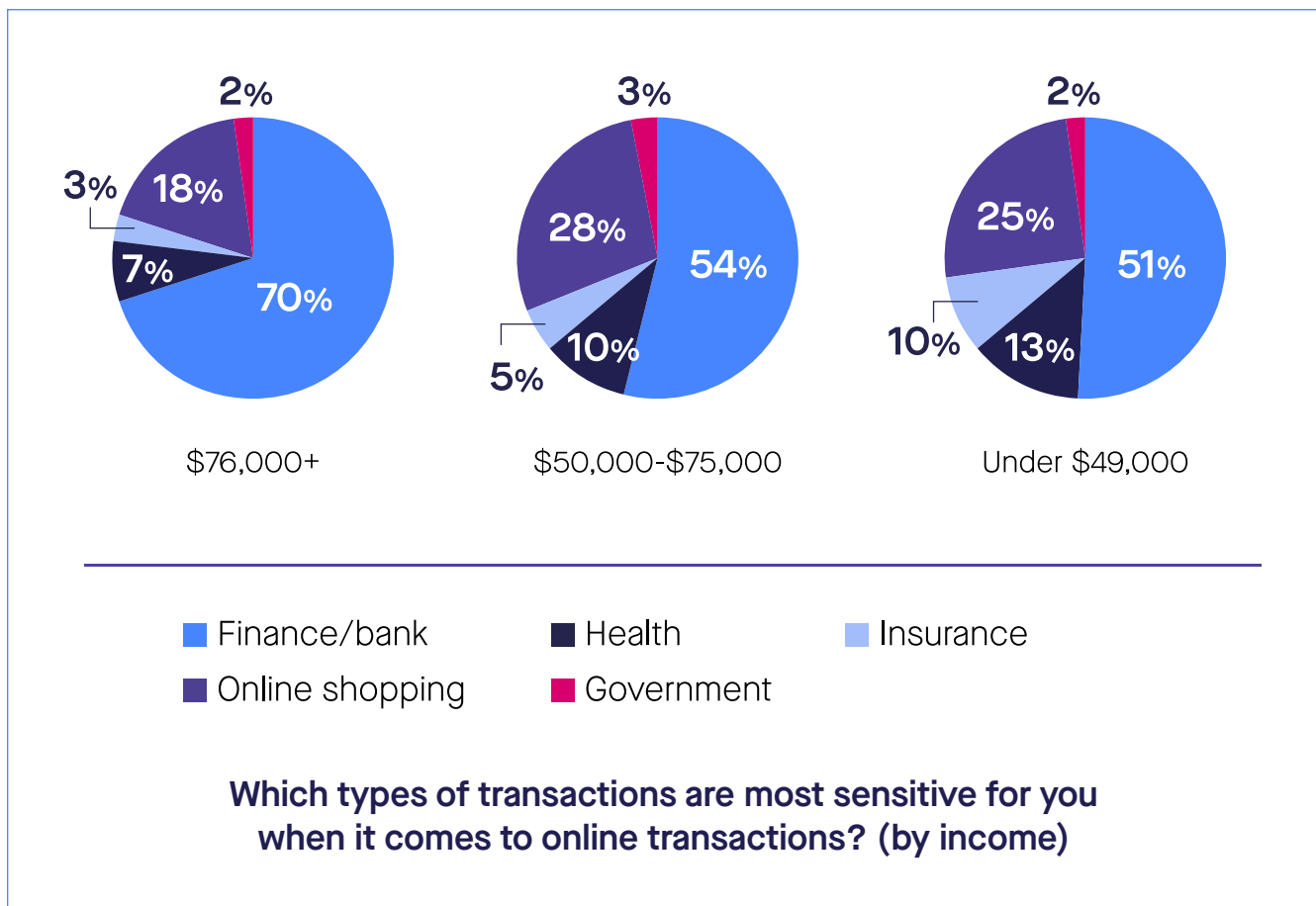
## Safe Digital Banking Is Paramount For High-Value Customers

For higher-income earners, trusting their banks is a matter of course. These are individuals who have likely had positive or at least neutral experiences with their banks over the years, and may even have an ongoing relationship with a personal bank or financial advisor.

But higher-income banking customers also have more sensitivities surrounding banking since they depend on their banks to grow and safeguard their wealth.



## Digital Banking Sensitive for Higher-Income Earners



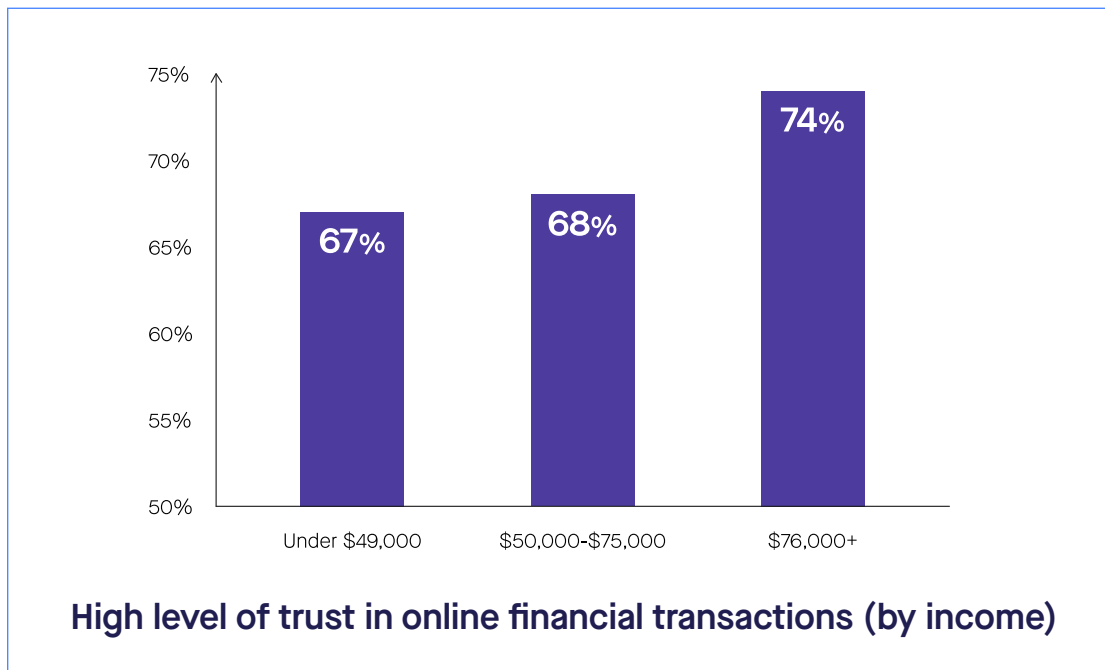
The higher-income earners in our survey (defined here as those that earn over \$76,000 a year) were significantly more likely to say that financial transactions are more sensitive to them than other types of online transactions. 70% rated financial transactions as the most sensitive, compared to just 51% of the lowest-income earners who said the same. When you have a lot, you have a lot more to lose and that translates into greater levels of sensitivity and worry.

If banks want these individuals to use digital banking for high-stakes activities such as transferring significant amounts of money or investing, digital channels need to be seen as equally safe to in-person banking. Otherwise, digital banking will be relied upon for not much more than the most basic of tasks.



## A Matter of Trust

Here's the good news: The higher the customer's income, the more likely they are to trust digital banking. 74% of higher-income earners say they have a "high level of trust in online financial transactions," while just 67% of lower-income customers say the same.



But this trust cannot be taken for granted. Higher-income earners' sensitivity to financial matters means that even the appearance of lax security may cause them to shy away from digital banking when it comes to important matters like opening an account or transferring large sums of money. Banks that invest significant time, effort, and funds in setting up digital infrastructure will not see the expected ROI if their most desirable customers hesitate to fully embrace digital banking due to security concerns.

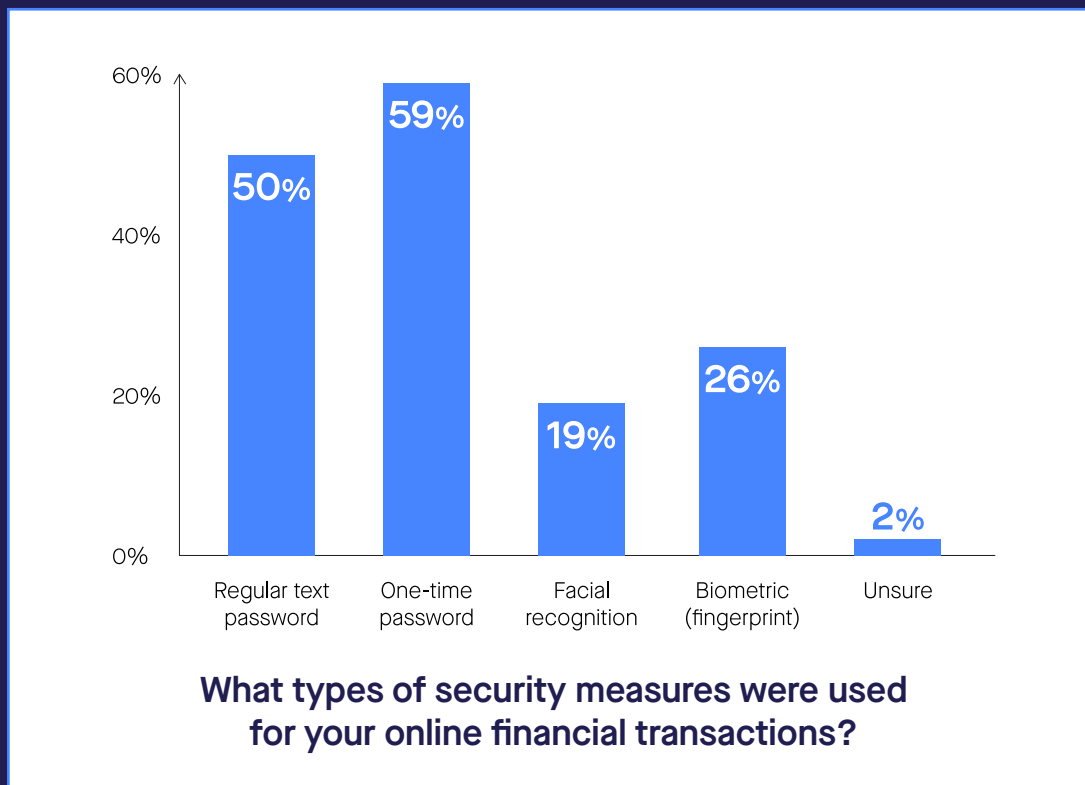
Indeed, the survey reveals that higher-income customers continue to perceive in-person banking as the most secure environment. This suggests that in-person banking is still widely regarded as the gold standard when the financial stakes are higher. For banks that want to meet their higher-income customers' standards, they will need to continue to invest in visible security features. At the same time, these customers should be able to complete security checks from a single channel without being bounced around.

## Part 4

# Cumbersome Digital Security is Costing Banks Heavily

Our survey also sought to discover which types of security measures customers encounter the most during digital banking sessions, and how it impacts their customer experience.

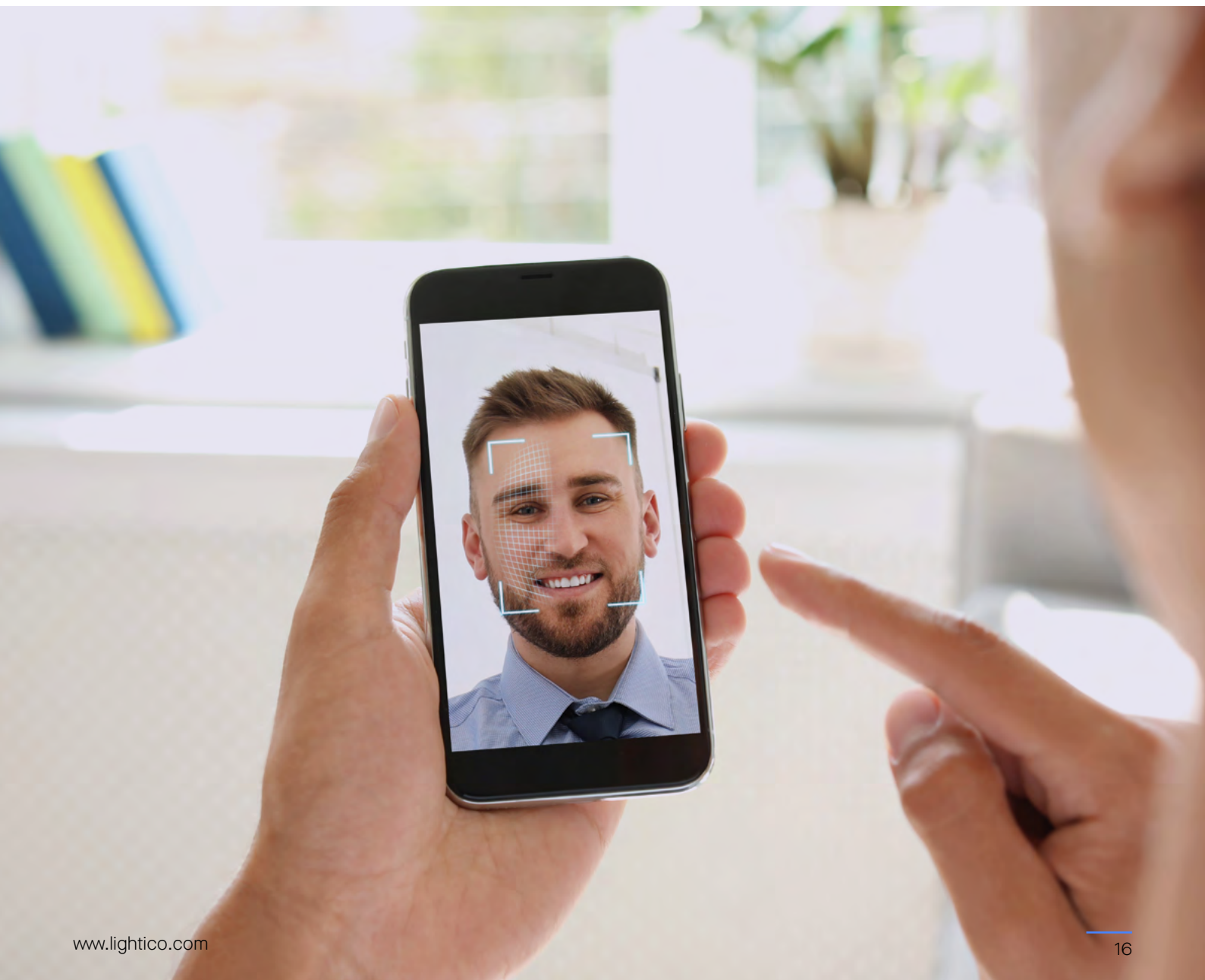
By and large, consumers most frequently encounter text-based passwords.



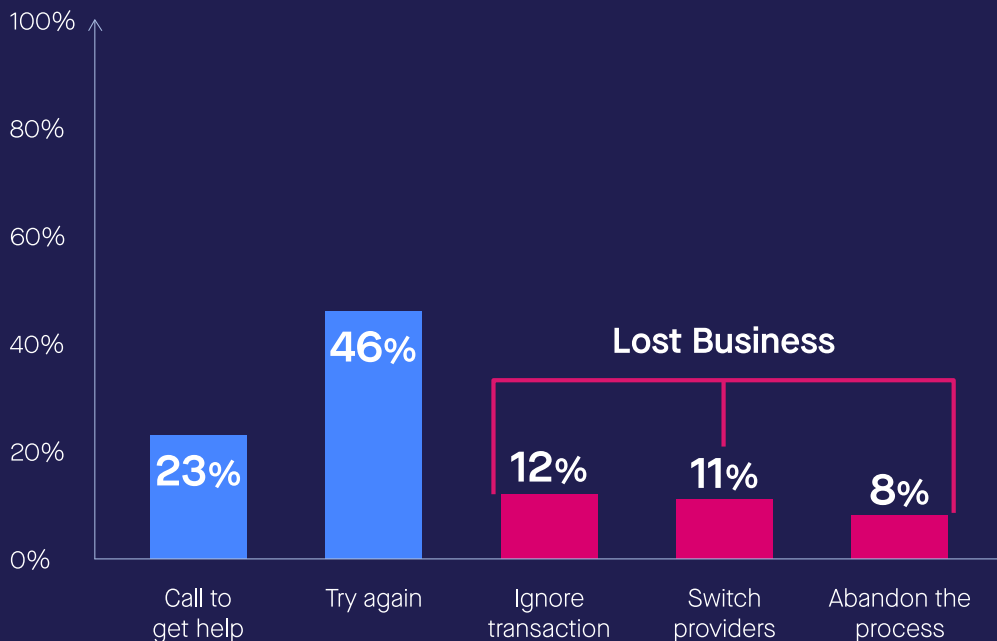
One-time passwords (OTPs) are particularly prevalent, with 59% of consumers saying they've been asked to use them during their recent online financial transactions. OTPs are advantageous security-wise because they aren't vulnerable to replay attacks; they are random and work for a single session only.

Regular text passwords are also commonly encountered at a rate of 50%. To lessen the probability of phishing attacks, banks often require customers to change their password every few months. Unfortunately, this causes friction as customers must keep track of constantly changing passwords, many of which have complex requirements.

**59% of customers have recently encountered one-time passwords when banking online. Just 19% have encountered more intuitive facial recognition-based logins.**



## More than 1 out of 4 online transactions with access issues are lost, almost half of those switching providers

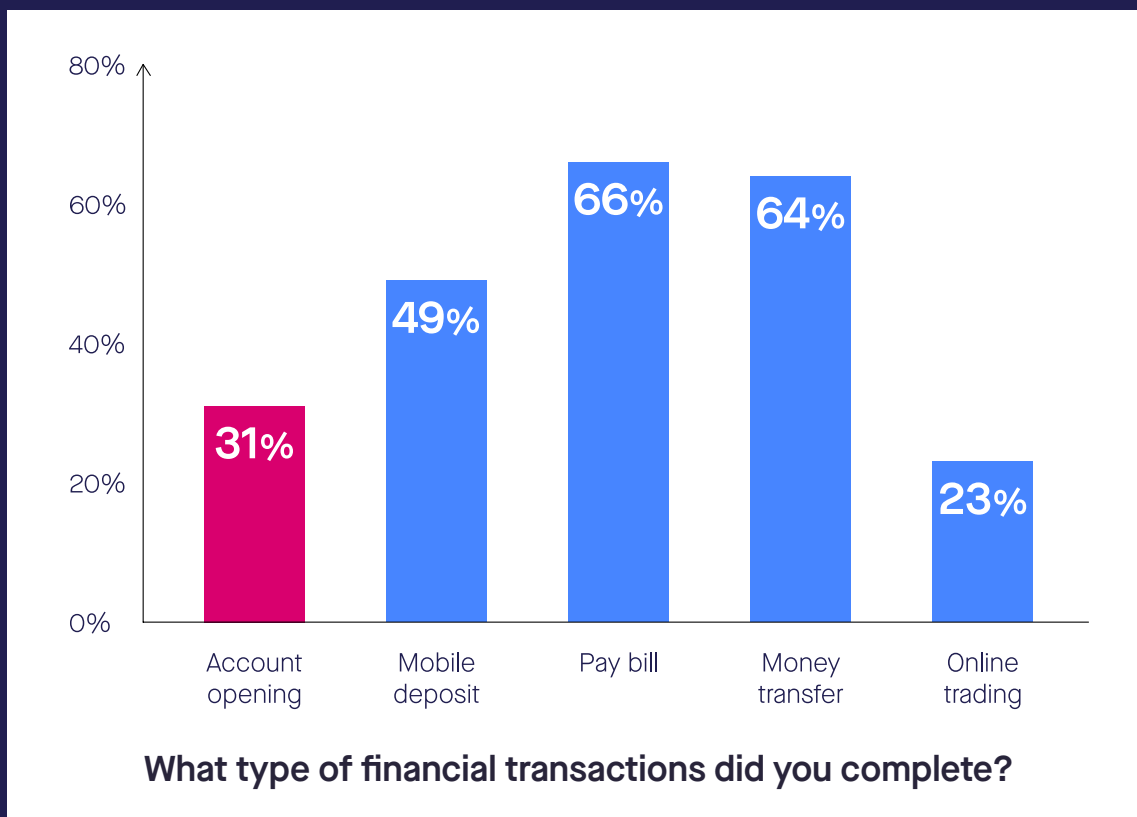


### What do you do when you have problems completing a login/password/check?

Complicated and ever-changing passwords, along with CAPTCHA and other security checks, are a frequent cause of access issues. For example, customers who fail to correctly enter their password after several attempts may be blocked from trying again within a certain period.

When customers fail to access their accounts, 46% try again to gain access, though there is inevitably a limit to their persistence. 23% call a customer support hotline to get help. More concerning, 12% simply ignore the transaction, 11% switch providers, and 8% abandon the process. In other words, more than one in four online transactions with access issues are lost, with almost half of those leaving the financial institution altogether.

**More than 1 in 4 online transactions with access issues are lost.**



Many of these lost transactions are related to servicing, such as paying bills, transferring money, making a mobile deposit, or online trading.

But a sizable number are connected to opening an account. 31% of consumers say they have opened a financial account online in the past three to six months. Customers who face cumbersome security measures during the onboarding process never even get a chance to become paying customers, representing the most painful lost opportunity of all.

A Forrester study found that over 64% of banks report lost revenue due to problems in their onboarding processes. When they scratch the surface, they'll find that many of these onboarding issues come down to unwieldy security and compliance measures that thwart customers from easily opening accounts and receiving important services.

Considering that the average banking customer lifetime value is \$45,600 (for a customer lifespan of eight years, and both business and personal accounts), each prospective customer lost represents a sizable blow to revenue.



## Part 5

# More Seamless Security Requirements Needed

Both customer concerns about security and excessive friction due to security can cause banks to miss out on opportunities. The good news is that banks don't need to choose between security and ease of use.

Many of today's cutting-edge security measures fit seamlessly into customers' journeys rather than disrupt them. Yet they go woefully underused.

For example, biometric fingerprint and facial recognition logins promote high levels of security without the hassle and access issues characteristic of text passwords. These types of effortless login systems should be more readily adopted and promoted to customers as the default form of access.



Banks that want their customers to feel comfortable with digital banking for a wider range of activities will need to ensure the website or app itself exudes an air of seamless security. Site seals, security logos such as an SSL certificate, and clear, contextual explanations of security guarantees before the activity commences will reassure customers that they are in safe hands.

In addition, embedding security features such as photo ID verification, digital signatures, and PCI-compliant payments into key touchpoints enables customers to complete digital banking tasks securely and seamlessly.

Finally, digital banking should stay online. Allowing customers to begin banking processes online, only to have them fill out and submit physical forms through legacy channels adds detrimental levels of friction. By keeping processes fully digital and intuitive, customers can conduct end-to-end digital transactions with minimal disruption and maximum peace of mind.

In this way, non-intrusive security measures allow banks to maintain or even grow their profit margins through digital channels.



## Conclusion

# Investing in Customers' Peace of Mind and Ease of Use

As we've seen, banks that invest in digital infrastructure for more complex banking tasks may not be receiving the ROI they were hoping for. This is particularly the case for higher-income and senior citizen customers who require extra reassurance.

If customers don't feel that their digital banking options are secure, they may postpone the transaction. They may also have an increased probability of switching over to a bank that they trust to provide the secure digital banking experience they seek.

And if customers don't feel that digital banking is convenient, if login friction or transaction friction is getting in their way of onboarding or getting serviced, retention will also be at risk.

The coronavirus has accelerated long-standing digital trends in banking. But to ensure that customers trust digital banking for all their needs, and not just rudimentary transactions, banks will need to ensure security measures are visible as well as non-intrusive. The most advanced automated and AI-based security features should be integrated seamlessly into customer journeys, ensuring digital banking fulfills its original promise of ultimate convenience.

Lightico enables insurers to accelerate and improve banking processes through end-to-end, mobile-first eSignatures, eForms, ID verification, and evidence collection. Our customers on average see 33% faster onboarding, 67% lower abandonment, and 25% increased conversions.





*“Lightico has really changed the game for us in being able to make digital banking more convenient for our customers. We can now collect multiple signatures on new account applications in under two hours - often within 45 minutes - and 90% are fully complete.”*

**- Stacie Smith, Vice President, Happy State Bank**



# Learn how Lightico can streamline your banking processes.

Try the interactive experience



Lightico

First Name: Jane

Last Name: Doe

Phone: 432 536 0001

Email: janedoe@gmail.com

Signature: *Jane Doe.*

SUBMIT

## About Lightico

Lightico's next generation platform for digital customer interactions empowers your agents to collect forms, documents, e-signatures, photos, consent to disclosures and to verify ID instantly while they have customers on the phone.

By simplifying customer interactions in the last mile of the customer journey, businesses make it easier for their customers to be their customers, earning their trust and loyalty, translating to higher profits.

275 7th Ave.  
New York, NY 10011  
[www.lightico.com](http://www.lightico.com)

Contact Information:  
1-888-252-1440  
[info@lightico.com](mailto:info@lightico.com)







Copyright © 2020 Lightico Ltd. All rights reserved.

visit: [www.lightico.com](http://www.lightico.com)