Eckoh

Banking Industry Report 2024

Hitting Home:

How Secure is the Home Contact Center?

Crucial insights for the banking sector

Customer retention is more critical than ever. Factors like global economic uncertainty and high interest rates are adding additional pressure in a sector that is already fiercely competitive. We see fintech players and modernizing incumbents all battling for customers that have never had so much choice. Banks need to find ways to forge deeper customer relationships and increase customer loyalty.

Our latest research highlights a crucial aspect of this: consumer security concerns about interacting with banks that employ work-from-home (WFH) contact center agents.

Security concerns

43% of consumers believe it is unacceptable for WFH agents in the banking sector to handle payment information or personal data, **the highest of any sector covered in our research.**

Consumer sentiment

A further 33% demand that banks provide clear evidence of extra security measures in place for it to be acceptable.

Take Five

76% of customers raise significant concerns about engaging with banks that have contact center agents working at home.

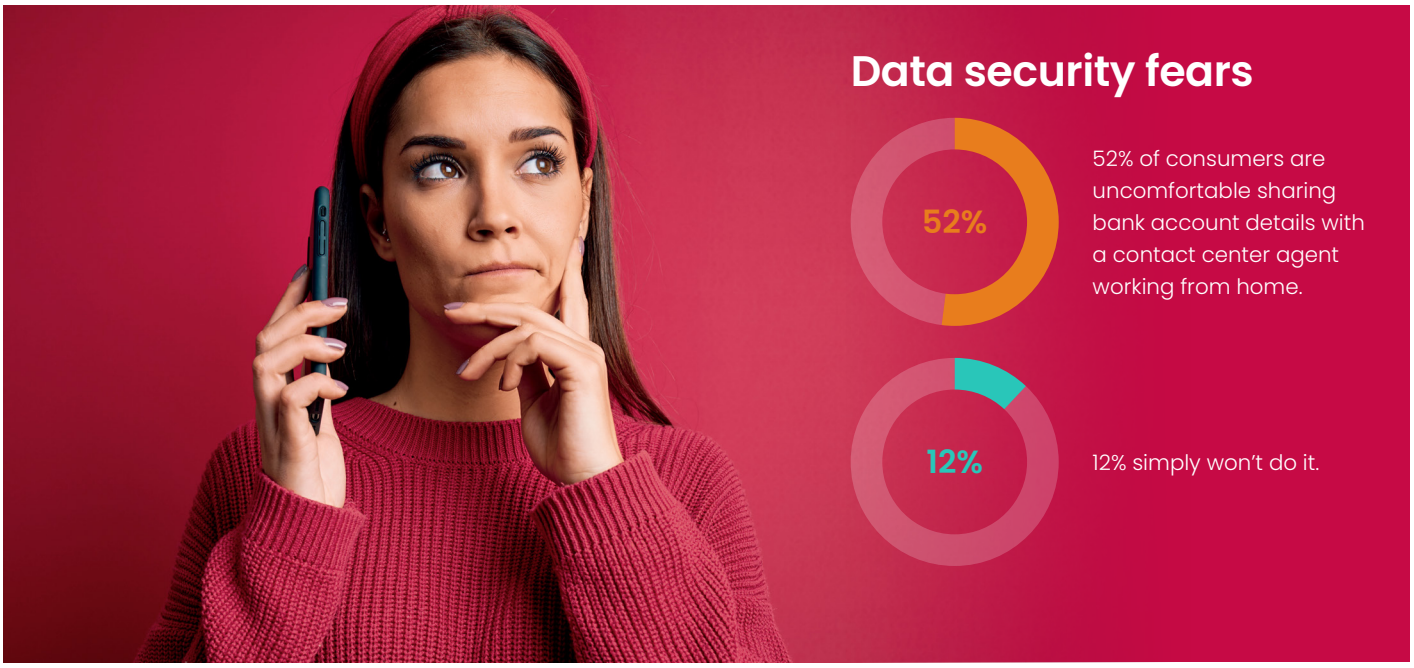
64% of consumers are uncomfortable sharing bank account details with acontact center agent working from home, while 60% are uncomfortable sharing their social security number.

54% would either walk away or consider walking away from a relationship with their bank if it became apparent that a contact center agent working from home was not in a completely secure environment.

78% want their banks to be more open about the security measures in place to protect payment information and personal data.

Consumers find the ability to input personal information and payment data using their phone's keypad while on the call with the agent the most reassuring measure.

Eckoh



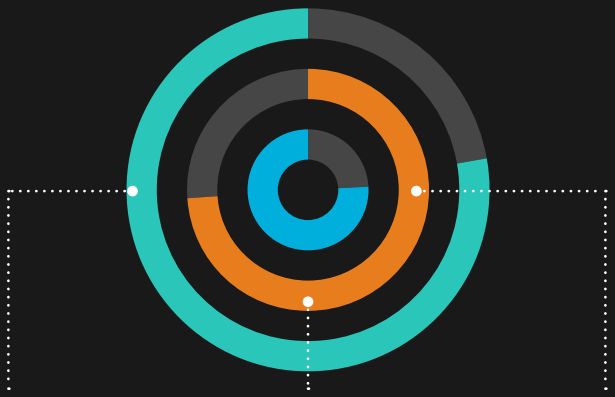
Data security fears

52% of consumers are uncomfortable sharing bank account details with a contact center agent working from home.

12% simply won't do it.

A wake-up call for banking sector leaders

The banking sector is already addressing rising cybersecurity risks and working to reassure customers that they have the right measures in place to protect their data and transactions. Our research highlights that they cannot afford to ignore the contact center experience.



Security protocols: 78% of consumers expect openness about the security protocols protecting their payment and personal data.

Transparency is key: 74% of consumers want banks to be upfront about employing WFH contact center agents.

Trust through robust measures: 76% of consumers are more likely to engage with banks that implement and disclose robust data security measures.

Essential steps for Banks

To effectively respond to these consumer demands, banks must focus on three key areas:

1. **Transparency & disclosure:** Being honest and open about WFH practices and security measures in place.

2. **Investment in technology:** Implementing the right technology to enhance data security.

3. **Reimagining relationships:** Developing a new approach to managing and supporting WFH agents.

Discover how you can safeguard your business by downloading our full report here

In today's competitive landscape, can you afford not to take these steps?