

---

# SECURING THE DIGITAL BANKING EXPERIENCE

## Striking a Careful Balance Between Banking Security and the Customer Experience

*"Companies need to secure their digital channels against malicious attackers – without creating a negative experience for their customers."*

*- McKinsey & Company<sup>1</sup>*



Banking customers are rapidly gravitating towards digital channels. To meet this growing demand, banks are working hard to expand and scale their digital offerings. Sensing an opportunity to exploit changing consumer behaviors and vulnerable systems, cybercriminals and fraudsters are increasing the breath and frequency of their schemes.

Today's banks are tasked with providing superior customer experiences while also addressing growing security threats and complying with challenging regulatory frameworks. To remain competitive, banks must find the perfect balance. Too much security produces a fragmented customer journey. Too little can result in devastating financial and reputational damage.

Many financial institutions are finding this balance in the cloud. Innovative solutions such as a unified communications platform helps banks to scale their digital transformation initiatives while leveraging a powerful and secure infrastructure.

---

<sup>1</sup> Bailey, Tucker, et al. "Building Security Into The Customer Experience." 29 June 2020, <https://www.mckinsey.com/business-functions/risk/our-insights/building-security-into-the-customer-experience>

---

## THE GROWING DEMAND FOR DIGITAL

While the use of mobile and digital banking channels were already on the rise, the COVID-19 crisis has accelerated customer demand for a robust digital experience. According to a recent survey<sup>2</sup> of 6,000 U.S. banking consumers:

- **27% of respondents** reported that the pandemic has made them more likely to use their bank's website.
- **23% of respondents** said that the pandemic has made them more likely to use their bank's mobile app.
- **26% of respondents** reported the same about online mobile payment apps.
- **Approximately 25% of respondents** said they are less likely to visit their bank's branch offices.

The survey also found that "Millions of banking relationships are up for grabs," with **14% of consumers** stating that they are likely to switch their primary bank in the next 6 months. **Approximately one-third** of this group said that, prior to COVID-19, they had not been considering a move.

With the rapid push towards all things digital, cyberattacks against banks are on the rise. Research<sup>3</sup> from a leading cybersecurity firm that examined cyberattacks during the pandemic found:

- A **238% surge in cyberattacks** against banks during the pandemic.
- **80% of CIOs** at major financial institutions reported a greater number of cyberattacks over the past 12 months.
- **82% of CIOs** said that cybercriminals' techniques appear to be improving by moving beyond the human factor to target weak links caused by processes and technologies in banks' supply chains.

Banks are under more pressure than ever to adapt to changing customer needs while guarding against increasingly sophisticated security threats. Overcoming these challenges involves striking a careful balance between security and a seamless customer experience.

---

<sup>2</sup> S PWC. "Many Consumers Think Their Banks Are Doing A Good Job. In A COVID-19 World, Will That Be Good Enough?" <https://www.pwc.com/us/en/industries/banking-capital-markets/library/consumer-banking-survey.html>

<sup>3</sup> VMWare Carbon Black. "Modern Bank Heists 3.0." May 2020, <https://www.carbonblack.com/resources/modern-bank-heists-2020/>

---

## DESIGNING A SECURE CUSTOMER JOURNEY

*“Leading companies are stepping back to think about designing a secure customer journey – that is, a relatively engaging online and mobile experience for legitimate users that is also safe from cyberattacks and fraudsters.”*

*- McKinsey & Company<sup>4</sup>*

Imagine for a moment that you are a banking customer. You just logged on to the online system to view recent transaction history. You notice a pending charge from an unfamiliar merchant and would like additional information to verify the transaction. At this point, you could pick up the phone and call the bank, but you want to avoid the time and hassle of a lengthy wait and authentication process.

Like most customers, you prefer to utilize a secure digital channel to get a quick answer to your question. You elect to initiate a chat directly from the bank’s homepage. However, once you open the chat window a prominently displayed disclaimer instructs you not to submit any sensitive personal information (i.e., account number or social security number) over chat since it is not secure.

You are then prompted to submit your contact information and wait to receive an email with a link to a secure chat. What should have been a routine inquiry in an increasingly digital world has turned into an unpleasant online banking experience. And while this fragmented interaction may seem like a mere speed bump in the much larger customer journey, the costs of a single bad banking experience are enormous.

In fact, a recent large-scale consumer benchmark study<sup>5</sup> involving 10,000 U.S. consumers found that, “Although only 6% of customers who interacted with a bank over the previous six months say they had a bad experience, of those customers who did have a negative interaction, **42% of them** say they either decreased spending or stopped spending with the bank after that poor experience.”

---

<sup>4</sup> Bailey, Tucker, et al. “Building Security Into The Customer Experience.” 29 June 2020, <https://www.mckinsey.com/business-functions/risk/our-insights/building-security-into-the-customer-experience>

<sup>5</sup> Zdatny, Isabelle. “10+ Years Later: How Customer Experience Has Shaped The Banking Industry.” 20 Feb. 2020, <https://www.forbes.com/sites/sap/2020/02/20/10-years-later-how-customer-experience-has-shaped-the-banking-industry/?sh=4aeec4c3bd8c>



That is not to say that some level of friction in the customer journey is not to be expected. Financial institutions face complex and dynamic regulatory frameworks that require the adoption of complicated risk management systems. These systems often result in rigid business processes that trickle into the customer experience.

Research suggests that banking customers are willing to accept some level of friction in digital banking transactions if it means safeguarding their sensitive personal information. For instance, research by Experian<sup>6</sup> found that **66% of consumers** say that they appreciate security “hurdles” because it makes them feel better protected. Yet even the most security conscious of banking customers can quickly tire of restrictive measures, particularly when it comes to ease of communication.

Returning to our hypothetical for a moment, the bank could have improved the customer experience by simply deploying a secure chat feature directly on their website. Rather than waiting to receive an email, you could have shared your information immediately through chat with the reassurance that it was secure.

Designing a secure customer journey requires a multifaceted approach that balances security, the user experience, and compliance. By strategically deploying secure solutions across all digital channels banks can provide consistently great customer experiences.

---

<sup>6</sup> Experian. “The 2018 Global Fraud and Identity Report. 2018, <https://www.experian.com/assets/decision-analytics/reports/global-fraud-report-2018.pdf>

---

## LEVERAGING SECURE CLOUD-BASED COMMUNICATION SOLUTIONS



*"Our survey found that outperforming banks are 88 percent more likely to include hybrid cloud adoption as part of their overall business strategies and 34% more likely to deploy cloud to increase operating margins."  
- IBM Institute for Business Value <sup>7</sup>*

To satisfy rapidly growing consumer demand for digital banking experiences, financial institutions are increasingly relying on third-party solutions. This often proves counterproductive. While banks are increasing their digital offerings, disparate systems can produce friction in the customer journey. Moreover, a growing vendor network presents unique security and risk management issues.

Growing concerns over third-party handling of customers' personal information has led to strict new regulations that require financial institutions to implement comprehensive risk management processes. For example, banks must exercise due diligence when selecting third parties and are responsible for the ongoing monitoring of their activities.

The direct and indirect costs of managing large vendor networks are substantial. Conducting due diligence on dozens or even hundreds of vendors necessitates large compliance teams. A third-party security incident can have a devastating financial impact on a bank. As a practical matter, regulators, the media, and customers draw little distinction between internal security incidents and those involving third parties.

A unified communications (UC) solution helps financial institutions to provide secure customer experiences while minimizing risk and increasing compliance. First, banks can provide a superior digital experience without the need to rely on large vendor networks since a cloud-based UC solution provides a robust choice of encrypted messaging options.

---

<sup>7</sup> IBM Institute for Business Value. "Tailoring Hybrid Cloud For Banking: Designing the Right Mix for Innovation, Efficiency, and Growth." 2017, <https://www.ibm.com/downloads/cas/74KLAO6J>

---

Second, banks eliminate the need for costly and time-consuming third-party risk management programs. Moreover, they reduce their exposure to potential third-party security incidents. Third, an industry leading UC solution will include best-in-class security features. This allows financial institutions to leverage the UC provider's infrastructure and expertise to safeguard customer data.

A UC provider's full-time job is to ensure the security of communications. A financial institution's conventional in-house system, however, involves many IT concerns, of which security is just one part. According to research,<sup>8</sup> some **94% of organizations** experience an improvement in security after switching to the cloud, while **91% report** that cloud-based solutions simplify government compliance requirements.

## CHOOSING A UNIFIED COMMUNICATIONS SOLUTION

With so many options to choose from, how can you be sure that a UC provider is the right choice for your bank? First, make sure that the provider has a proven history of serving the banking industry. Financial institutions face unique challenges. Choosing a UC provider that understands the banking customer journey, security challenges, and regulatory frameworks is crucial.

Second, find a provider that has achieved and maintains the highest security standards in the industry. For instance, a HITRUST certification means that an organization as well as all its products has undergone rigorous scrutiny and is a verified-secure partner whose technology banks can leverage to drive digital transformation.

As financial institutions continue the transition to all things digital, they will continue to face dynamic and sophisticated security challenges. In responding to these challenges, banks must not lose sight of the customer experience. A unified communications solution can help banks to strike the perfect balance and gain an edge over the competition.



---

<sup>8</sup> Rapidscale. "Cloud Computing Stats – Security and Recovery." <https://www.slideshare.net/rapidscale/cloud-computing-stats-security-and-recovery>

# ABOUT REVATION SYSTEMS

At Revation Systems, we have a passion for making the complex simple and embracing risk to deliver great results. We have a security-first mindset and a purpose-built approach to everything we do from our policies and processes to our infrastructure and architecture. Security is at the core of our DNA; both at the organizational level and for the architecture of our technology. Security is not a check box for us, but rather an approach that starts from the ground up and influences every product we bring to market. We take the hard road every time to ensure our customer's data — in the two most tightly regulated markets — remains protected.

Our secure solutions have been validated with our HITRUST Certification. For financial providers, HITRUST certification means that the organization in question (including its products) has already undergone rigorous scrutiny and is a verified-secure partner whose technology and organization could leverage for its digital transformation without fear, hesitation, or time spent on an additional internal review.


We believe in the power of human relationships and that innovation in communication will connect people to help achieve financial security and live healthier lives. Revation Systems serves hundreds of healthcare and finance consumers in the U.S. with its all-in-one full contact center in the cloud with the ability to drive experience across digital and physical channels. LinkLive is unified communications software hosted in the cloud that offers a broad range of capabilities including rich digital messaging, a seamless ability to engage humans across physical and digital channels, and leading voice and video communications.

We offer the advanced, sophisticated capabilities are expected in a contact center like skills-based routing, session recording, workforce management, agent scheduling, and quality monitoring tools. We also offer a broad range of digital capabilities from chat, secure mail, and co-browsing to the ability for digital users to engage the physical channels and humans at a healthcare or banking organization. Since its founding in 2003, Revation has been dedicated to the belief that the quality of communications can be increased, while the costs and hassles can be decreased, using virtual communications with a cloud-based platform.

**Have Questions?  
Let's Connect!**


[Click Here](#)

#### MINNEAPOLIS

 225 S 6th Street, Suite 3900,  
Minneapolis, MN 55402

 1.952.392.1834

#### SAN FRANCISCO

 535 Mission Street - 14th Floor,  
San Francisco, CA 94105

 1.952.392.1834

CLICK ON ONE OF THE FOLLOWING  
TO LEARN MORE ABOUT US!

  [WWW.REVATION.COM](http://WWW.REVATION.COM)