balancing fraud prevention and user experience in digital applications

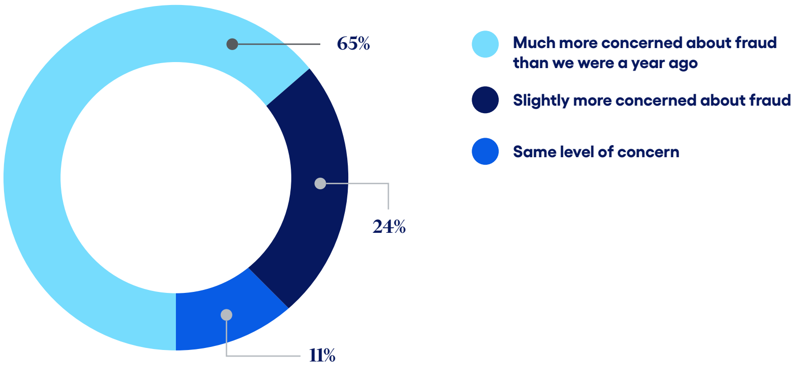
Digital account opening solutions have emerged as one of the most essential initiatives a financial institution should invest in. In fact, account opening has consistently been a very hot topic in Cornerstone's What's Going on in Banking report for the past four years.[1]

However, many banks and credit unions are still hesitant about the digital account opening channel. Financial institution leaders have to weigh the potential for more applicants against a projected increase in operational costs to perform manual reviews and the possibility of new fraud.

65% of respondents are much more concerned about new account fraud in the digital channel than they were just one year ago.[2]

How would you characterize your bank's level of concern about fraud in its digital channels this year versus last year?

Respondents were asked to choose the statement that best describes their bank.



These concerns are valid. According to Alloy's latest fraud benchmark report, 54% of financial institutions have lost over $500K in direct fraud losses in the last 12 months, and 25% of respondents lost over $1M in direct fraud losses over that same span.[3]

The stakes for fraud are higher than ever. A majority of decision-makers agree that the related financial, reputational, and compliance risks associated with fraud are growing. The key to solve these unsettling trends is to find the right balance between a successful fraud prevention program and providing a seamless applicant experience. Technology can provide a bridge that satisfies both needs.

54% of financial institutions have lost over $500K in direct fraud losses in the last 12 months.

overcoming application abandonment

For budget-conscious or resource-constrained community and regional financial institutions, manually reviewing every account application and closely inspecting documents isn't the best use of employees' time or talents.

Not only is manual decisioning expensive and time-consuming, but accountholders experience delays while their information is being processed – which can cause them to abandon their applications and open accounts elsewhere. 49% of consumers report abandoning their online applications due to an organization requesting too much information.[4]

49% of consumers report abandoning their online applications due to an organization requesting too much information.

So, what's the best way to remain compliant and efficient, while increasing the number of online account openings? A modern application interface, coupled with technology that automates the identity verification process. Using multiple, specialized data sources makes it easier to acquire more qualified applicants while dramatically decreasing both manual review time and costs.

Here are some best practices to help you achieve the right balance:

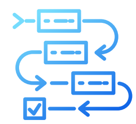
1. **Implement an end-to-end solution for digital account onboarding:** Streamline account opening platforms, fraud prevention, and KYC checks into a unified, automated solution to balance a seamless accountholder onboarding experience with robust risk management controls.

2. **Look for a modern origination system with open APIs and tight fintech integrations.** With these, you'll be able to integrate the best identity verification and funding tools available while maintaining a smooth connection with your core provider.

3. **Layer multiple data sources for a complete view of accountholder identity:** You'll see the best success by layering multiple layers of identity data products into your decisioning workflow. Sometimes referred to as the "Swiss Cheese Model" to fraud prevention, each layer has potential vulnerabilities or "holes," similar to a piece of Swiss cheese. However, when you align them strategically, the likelihood of fraudsters getting through all the layers diminishes.

4. **Centralize accountholder onboarding data in one location:** Data orchestration tools help streamline all of your accountholder identity data into a single identity risk profile for each of your accountholders. This eliminates data silos and allows your teams to look at each accountholder's risk holistically.

5. **Continuously optimize risk policies:** Fraud is always changing, and fraudsters are consistently looking for new vulnerabilities in the fraud controls of financial institutions. The controls you have in place today might not be suitable protection for the fraudsters of tomorrow. Savvy financial institutions invest in scalable fraud prevention technology that empowers quick workflow changes and helps avoid vendor lock by easily testing, adding, and changing new data sources.



Using multiple, specialized data sources makes it easier to acquire more qualified applicants while dramatically decreasing both manual review time and costs.

safeguarding and enhancing accountholder relationships

Investing in a digital account opening platform – coupled with a sophisticated and layered security approach – not only enhances the accountholder experience but can also drive substantial financial benefits for your institution. Allowing the good applicants in faster while keeping the bad ones out.

Using multiple data sources simultaneously also provides protection against bad or compromised data from any one source. Alerting you more quickly to potentially fraudulent account openings while protecting both your institution and accountholders.

ready to get started?

Get in touch with us to discuss developing a secure, digital account opening strategy today.

For more information about Jack Henry, visit jackhenry.com.

sources

1. Ron Shevlin, What's Going on in Banking 2024, Cornerstone Advisors, accessed January 2025.
2. 2024 Technology Survey, Bank Director, accessed January 2025.
3. 2024 State of Fraud Benchmark Report, Alloy, accessed January 2025.
4. H2 2024 State of Omnichannel Fraud Report, TransUnion, accessed January 2025.