protecting your digital front door: thrive in a digital-first world

Lead With Trust and Safeguard Accountholders

Fraud losses topped the list of CEO concerns in the Jack Henry™ 2025 Strategy Benchmark – a first in the survey's history.[1]

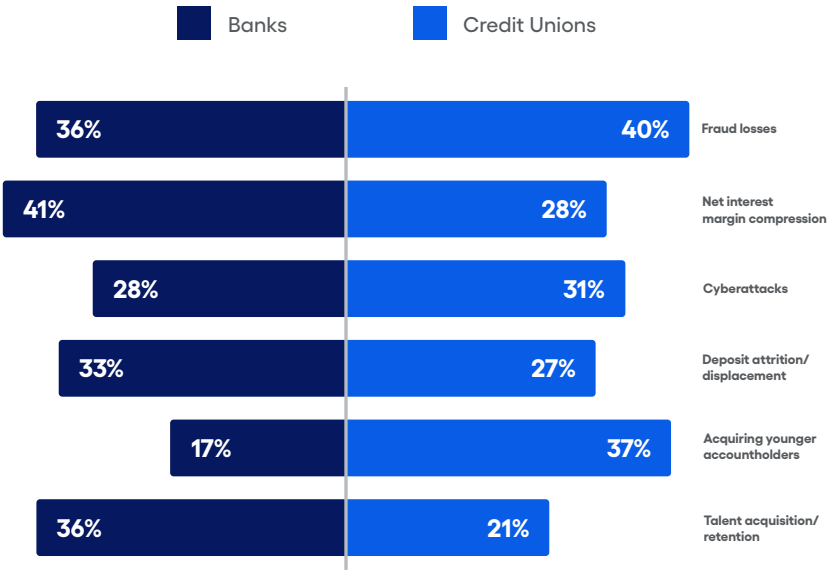
This shift reflects the rapidly evolving threat landscape and the growing urgency to protect accountholders from increasingly sophisticated attacks. In 2024, the U.S. led the world in scam-related losses, averaging $3,520 per victim.[2] More than 77 million adults have experienced an account takeover attempt or incident.[3] Synthetic identity fraud is projected to generate over $23 billion in annual losses by 2030.[4] And the FBI has reported a sharp increase in real-time payment fraud, which is particularly difficult to detect and stop.[5]

These numbers are more than statistics.

They represent real people whose trust in their financial institutions is on the line. Protecting them requires more than technology. It means taking a proactive, human-centered approach to security.

Top Three Concerns

Over the next two years, what are your top three concerns?



building trust through secure banking

Trust is built – or broken – at every touchpoint.

Mobile, online, in-branch, call centers, eCommerce, cards, and ATMs all play a role. Many consumers are concerned. In Jack Henry's second annual Financial Sentiment Study, 35% of consumers said they were dissatisfied with their primary financial institution's protection capabilities such as proactive advisory alerts and notifications, secure chat, security awareness and training, and stolen or missing card controls.[6]

This concern is a call to action.

Accountholders are actively seeking financial partners who prioritize their safety. That means integrating fraud prevention into digital experiences and other channels, not just as a technical safeguard but as a strategic differentiator. Features like proactive alerts, automated notifications, and in-app card controls are no longer optional – they're expected.

35% of consumers said they were dissatisfied with their primary financial institution's protection capabilities.

But technology alone isn't enough. It's also important to invest in education and awareness – helping accountholders recognize threats and respond with confidence.

strengthening accountholder trust through transparency

If fraud occurs, there's still a chance to build trust.

Helping accountholders understand what happened – and who was responsible – can make a lasting difference. When fraud is promptly and accurately resolved, it can deepen accountholder trust (often strengthening their loyalty more than if no fraud had occurred).

As Vamsi Kanuri, Marketing Professor at the University of Notre Dame, observed: "Surprisingly, when the bank catches the real fraudster, not only do customers feel more secure, but also 62% fewer leave compared with customers who never experienced fraud at all."[7] That's a powerful reminder that technology and empathy can turn moments of risk into lasting relationships.

It's proof that transparency and resolution can strengthen relationships – even in the wake of fraud.

enhancing digital banking UX with seamless compliance

Digital banking is central to consumers' financial lives.

That means banks and credit unions face the challenge of maintaining strict regulatory compliance without compromising user experience. Requirements like identity verification, fraud prevention, and data protection can introduce friction if not thoughtfully integrated. The solution lies in embedding compliance into the user journey through automation and intuitive design.

"When the bank catches the real fraudster, not only do customers feel more secure, but also 62% fewer leave."

Vamsi Kanuri
Marketing Profession at the University of Notre Dame

Requirements like identity verification, fraud prevention, and data protection can introduce friction if not thoughtfully integrated.

When done well, it not only reduces operational burdens, but it strengthens trust and satisfaction.

Compliance should feel seamless – not like a barrier, but like a safeguard.

using AI to stay ahead of banking fraud

Fraud tactics are evolving fast – and are getting harder to spot.

AI-generated forgeries, deepfake scams, and automated credential attacks are becoming more common. Financial institutions need to respond with equal sophistication. By using cloud-based platforms, AI, machine learning, and behavioral analytics, you can detect anomalies faster, prevent fraud before it causes harm, and reduce the strain on internal teams. Open integrations support smarter risk decisions and maintain trust in an increasingly complex environment.

In other words, you can stay ahead of threats without slowing down your experience.

preventing synthetic identity fraud

Synthetic identity fraud is tough to spot – but not impossible to stop.

This type of fraud involves creating fake personas using a mix of stolen and fabricated data. Advanced identity verification tools – like biometric checks and document authentication – help confirm that a person's identity is real and matches official records. By

More than 77 million adults have experienced an account takeover attempt or incident.

Synthetic identity fraud is projected to generate over $23 billion in annual losses by 2030.

blocking fraudulent accounts before they're opened, you can prevent downstream losses and protect legitimate accountholders.

Early detection means you can protect trust from the very beginning.

using secure messaging and chat for financial institutions

Convenience only builds trust when it's backed by security.

Conversational banking offers accountholders fast, convenient support without leaving the app. It reduces call center volume, improves service speed, and enhances the overall experience. But convenience must be matched with security. Secure authentication minimizes phishing risks, while modern chat platforms enable safe file sharing and transaction support.

By adopting open banking standards and secure APIs, you can replace screen scraping with smarter, safer data exchange.

securing real-time and digital payments

Faster payments means faster fraud.

The shift away from paper checks has made secure electronic payments a necessity for both consumers and businesses. But with speed comes risk. Push payment scams and business email compromise (BEC) schemes are increasingly targeting community financial institutions, often using deepfake technology to impersonate executives and authorize illegitimate transfers.

To stay ahead, financial institutions need to pair convenience with robust security. That means implementing layered fraud prevention – including AML and OFAC screening – and embedding identity verification into every payment experience.

It's how you protect every transaction – while giving accountholders the speed and convenience they expect.

Secure authentication minimizes phishing risks, while modern chat platforms enable safe file sharing and transaction support.

Push payment scams and business email compromise (BEC) schemes are increasingly targeting community financial institutions.

unifying fraud and risk strategy for financial institutions

Maintaining trust in today's fraud landscape requires a multi-layered strategy.

A scalable governance and risk platform that aligns regulatory needs with user-centric innovation is a necessity. Look for solutions that offer real-time, AI-powered fraud detection across multiple payment types. Ensure consistent experiences across your website and app and consolidate risk management and fraud prevention into a unified platform.

This approach supports both operational efficiency and accountholder confidence.

Maintaining trust in today's fraud landscape requires a multi-layered strategy.

ready to win the digital front door and secure your financial institution's future?

Download the full white paper to dive into ways you can attract, onboard, engage, and protect accountholders – while building lasting relationships.

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

sources

1. *2025 Strategy Benchmark*, Jack Henry, accessed August 5, 2025.
2. *International Scammers Steal Over $1 Trillion in 12 Months in Global State of Scams Report 2024*, Global Anti Scam Alliance, accessed August 5, 2025.
3. *Account Takeover Incidents are Rising: How to Protect Yourself*, Security.org, accessed August 5, 2025.
4. *Using Biometrics to Fight Back Against Rising Synthetic Identity Fraud*, Deloitte, accessed August 5, 2025
5. *Internet Crime Repot 2023*, Federal Bureau of Investigation, accessed August 5, 2025
6. *2025 Financial Sentiment Study*, Jack Henry, accessed October 28, 2025.
7. *Banks That Identify Fraudsters Increase Loyalty, Retain More Defrauded Customers Than Others Who Never Were Compromised*, Shannon Roddel, University of Notre Dame, Accessed October 6, 2025.