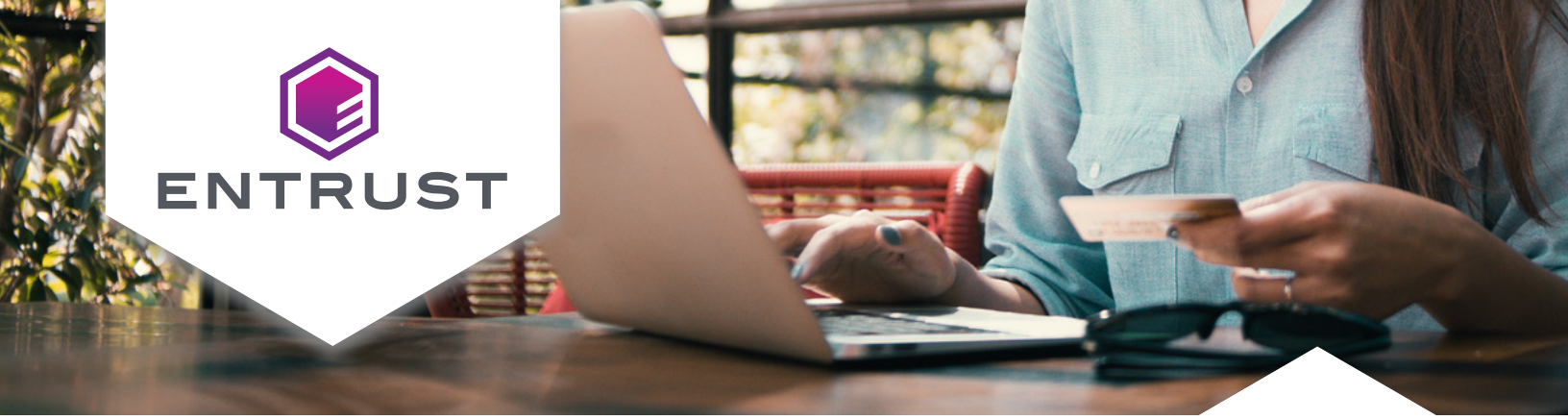


Fight Consumer Fraud with Entrust Identity as a Service

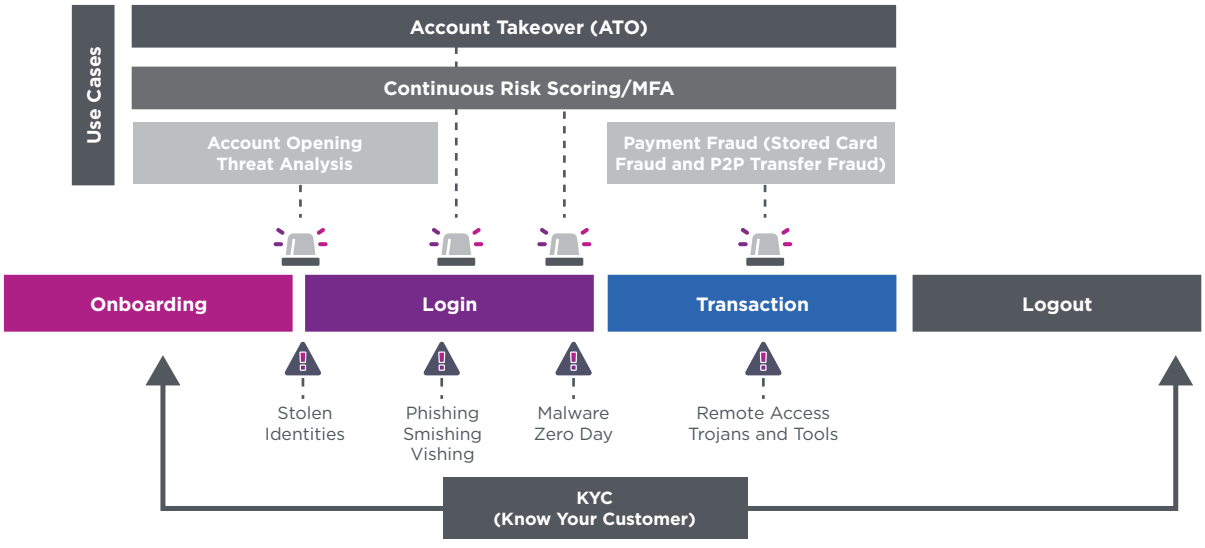
Online and mobile banking adoption has skyrocketed since the COVID pandemic started. In fact, according to the American Bankers Association, 71% of Americans are now relying primarily on digital channels for their banking needs. While this is largely good news for banks and credit unions, there remains a significant fraud challenge to address.

According to Aite Group, between 2019 and 2020, 47% of U.S. consumers experienced identity theft, 37% application fraud, and 38% account takeover.

Plus, Javelin reports global identity fraud losses topped $56 billion in 2020. From a financial institution (FI) perspective, mitigating fraud risk not only improves consumer trust, but also reduces fraud costs.

Fraud detection is good. Fraud prevention is better.

Detecting fraud for remedial action helps. But ideally, the goal should be fraud prevention. Entrust Identity as a Service (IDaaS) protects financial consumers across the financial service delivery cycle – from account opening and onboarding to transacting and logout – with our advanced AI-powered platform.



Learn more about Entrust IDaaS at entrust.com

Fight Consumer Fraud with Entrust Identity as a Service

Entrust IDaaS is an all-in-one solution that non-intrusively detects behavioral and environmental anomalies while protecting consumers from credential-stealing attacks, impersonation attacks, and computer/session-takeover attacks.

Key Capabilities

IDaaS protects consumers by thwarting would-be cybercriminals with:

Invisible Security: Behavioral biometrics and user behavior analytics identify bots and other suspicious patterns without impacting the consumer experience.

Secure Access: Monitors access network type and speed while protecting against an unauthorized change in access network. Protects against access from TOR Browser/Proxy networks as well as known fraudster locations.

Malware and Trojan Detection: Protects against malware designed to steal identity credentials or capture one-time passwords (OTPs). Protects and defeats remote access trojans that conspire to hijack user sessions.

Continuous Authentication: Behavioral biometrics and network and device data provide contextual awareness to continuously detect bad actors (including mule accounts), mitigating fraud risk regardless of attack type.

Automated Real-Time Response: Automatically stops active threats (i.e., malware, phishing, RATs, etc.) with pre-determined responses, including user notification, step-up authentication, session termination, and account lockout.

KEY BENEFITS

Reduce Fraud: Detect and respond in real-time to user impersonation and manipulation cyberattacks.

Reduce Costs: Minimize false alerts, fraudulent claims, and actual fraud losses.

Maintain Compliance: Protect consumer privacy, which is a core banking regulatory requirement.

Improve Security: Stop would-be cybercriminals from taking over accounts and/or creating new fraudulent accounts.

Create a Seamless Customer Experience: Continuously and invisibly verify consumer identities.

Protect Your Brand and Reputation: Build and maintain consumer trust by proactively keeping their identities and data secure.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223