BUSINESS GUIDE

AUTHENTIC ID

Moving at the speed of fraud.

360° Fraud Intelligence:
The Power of Multi-Layered Fraud Protection

Sophisticated fraud threats continue to grow. These fraud threats—from deepfakes and injection attacks to synthetic identities, and countless others—target businesses of all sizes and across all sectors.

These threats demand a robust, proactive, and multifaceted defense: layered fraud protection.

What Is Layered Fraud Protection?

If a bad actor gets through one security measure – your company's data and sensitive information (and its customers) could be at risk.

Layered fraud protection is the answer: multiple, interconnected security measures that work together to detect and prevent fraudulent activities at various stages of the customer journey. This approach minimizes vulnerabilities and ensures a higher level of trust and security for both your customers and your organization.

Why Your Business Needs Layered Fraud Protection

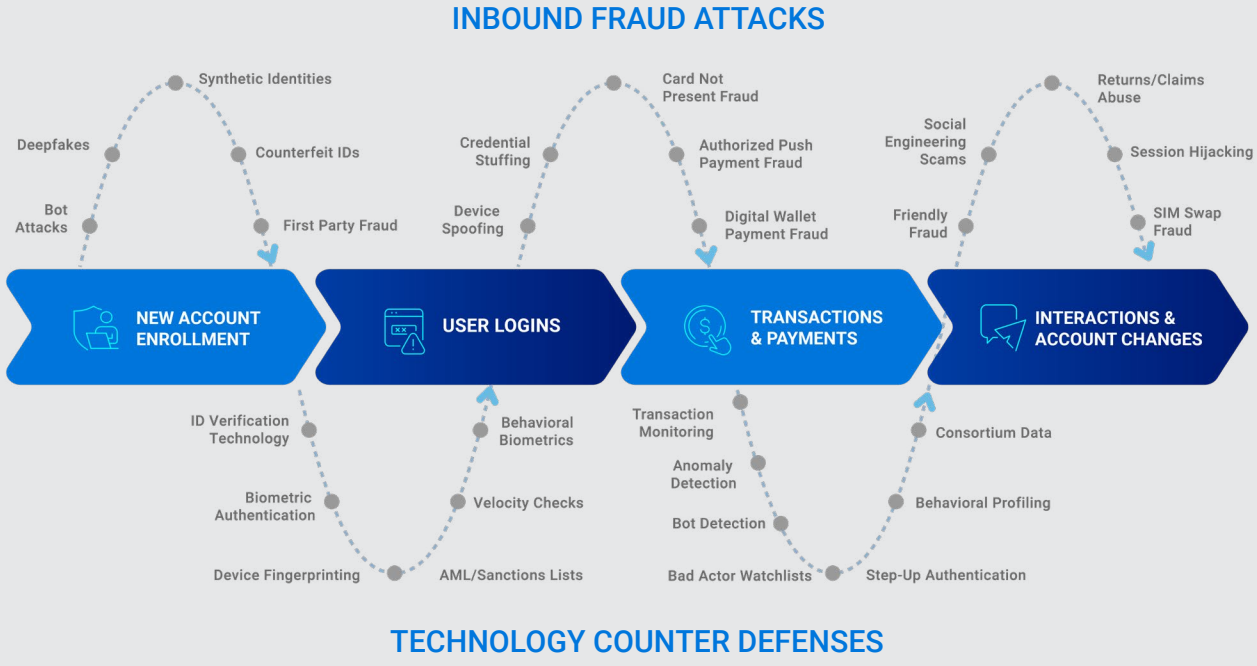
Relying on just a single security mechanism can leave critical gaps that fraudsters can exploit. A layered approach to fraud has many benefits for your business:

Omnichannel Coverage
Fraudsters often exploit gaps between channels (e.g., mobile apps, web portals, or in-person). Monitoring fraud across all touchpoints ensures coordinated defenses against sophisticated tactics.

Decisioning Accuracy
Reduce false positives and false negatives when you combine multiple layers, reducing the likelihood that legitimate customers will be flagged as potential fraud.

Adapt to Evolving Threats
Fraudsters constantly change tactics. Stay one step ahead with a layered approach that will ensure your defenses can evolve with changing threats.

Strengthen Regulatory Compliance
Your business may need robust anti-fraud measures to comply with data protection and financial regulations, like GDPR or AML. Meet these standards with layered fraud protection.



The Layers That Keep Your Business and Customers Safe

Document | ID Verification

Bad actors will often use stolen or fake identities to bypass your security protocols, especially during account opening and onboarding. ID verification tools use AI and machine learning to verify the authenticity of government-issued IDs and documentation by analyzing security features and fonts, among other items. With advanced ID verification, those IDs can be validated against authoritative databases for additional checks.

Biometrics with Liveness Detection

Biometric authentication adds yet another robust layer of security with minimal friction for users. With facial biometrics, your solution can match a selfie to a photo on a government-issued id, profile picture, or any other photo of a person's face with accuracy. Ensure your solution has liveness detection so your business can be sure the verification selfie is a real, present person, rather than a photo, 3D mask, or deepfake. These spoofing attacks are increasingly common.

Velocity Checks

Velocity checks monitor the frequency and pattern of transactions to evaluate fraudulent attempts that a bad actor attempts to initiate frequently in a certain (often short) timeline, which outlines a clear potential fraud pattern. Whether monitoring the rate at which an individual transacts or flagging multiple transactions that use the same headshot and/or selfie, you can reduce your company's risk of fraud.

Watchlists

Screen against watchlists to identify high-risk individuals before they enter your business' website or app and commit fraud. These lists can include anti-money laundering (AML) and politically exposed person (PEP) lists. Businesses can also enhance these lists with their own "bad actor" databases to further eliminate bad actors. Using updated information is a critical way to identify new threats and fraudsters.

The Layers That Keep Your Business and Customers Safe, *continued*

Behavioral Analysis

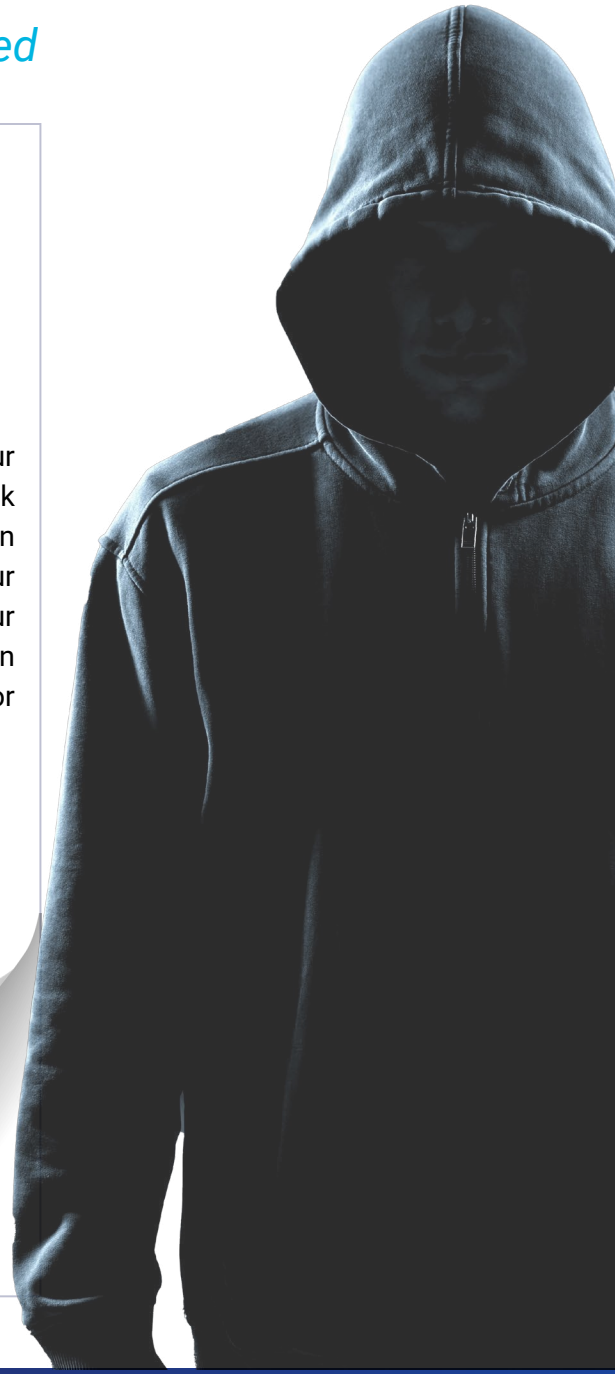
Legitimate users have largely predictable behaviors when opening an account or making a purchase online, and fraudsters don't. Use machine learning models to analyze this behavior to flag any suspicious activity. If a customer logs in from an unfamiliar location or device, it could indicate account takeover fraud activity and could be further assessed for more security protocols to protect your system.

Multi-Factor Authentication

MFA enhances security by requiring two or more proofs of identity: something you know (knowledge), have (possession), or are (inherence). Combining ID or mobile device authentication with biometric and behavioral analysis maximizes protection against a variety of threats.

Risk Scoring and Decisioning

With all the above data, your system should assign risk scores to each transaction or user action. With AI, your decisioning can allow your organization to take action in real time, including flagging or blocking suspicious activity.



How Layered Fraud Protection Keeps Fraudsters Out – and Your Costs Down

- **Earn Customer Trust**: Customers expect higher security than ever. If your customers know their data and transactions are secure, they're more likely to stay loyal to a secure brand like yours.
- **Cut Costs**: Preventing fraud will not only minimize your monetary spend each year, but it will also protect against the costly impact of breaches and other attacks.
- **Get Scalability**: A layered fraud protection strategy can scale with you as your business grows to ensure your security stays consistent.
- **Gain a Competitive Advantage**: Set yourself apart in a competitive marketplace with proactive fraud prevention.

Implement Layered Fraud Protection from AuthenticID Today

There's no silver bullet to stop fraud—that's why a layered fraud protection strategy is crucial. Your fraud protection strategy isn't just an investment in cybersecurity, it's an investment in the bottom line success of your organization.

Contact us today to safeguard your business with the platform trusted by the largest US banks, every major US wireless provider, federal agencies, and more.

AUTHENTIC ID

IDENTITY MADE SIMPLE

Visit **AuthenticID.com** to learn more or **schedule a demo**.