The 2026 **Fraud Prevention Handbook**

For Banks and Financial Service Providers

Top 10 financial fraud and cybersecurity challenges — and how to stop them

EBOOK

2024 set new records for financial fraud and cyberattacks — as did 2023, 2022 and most of the previous decade. Consumers around the world lost more than $1 trillion to scams, according to the Global Anti-Scam Alliance. Meanwhile, estimates suggest that financial service firms may have lost up to four times that amount.

So far, there's no indication that 2026 will be any different. In fact, Deloitte estimates that, by 2027, Generative AI and deepfake technologies could raise the losses consumers suffer from financial fraud to $40 billion in the United States alone.

From deepfakes and device clones to scams executed via phishing attacks, the shifting landscape of threats can be daunting. It simply isn't possible for financial service providers to eliminate the risk of fraud. But with the right combination of solution and approach, they can get the upper hand.

In this guide, we'll investigate the top ten types of attacks, explore how they're impacting banks and financial service providers — and examine the best ways to mitigate each risk.

1

Overview of problems and solutions

The Top 10 Types of Financial Fraud

1. Account opening fraud
2. Device cloning
3. Credential attacks
4. Brute force attacks
5. Account takeover fraud
6. Phishing, smishing and vishing
7. Authorized push payment fraud
8. Malware
9. SIM swapping
10. Insider threats

The Lifecycle of a Scam

The consumer banking journey runs from opening new accounts to logging in, transacting and initiating interactions that might deepen or expand the relationship. Fraudsters are with these consumers every step of the way, waiting to exploit any weakness or vulnerability.

That's why fighting fraud starts by evaluating the full lifecycle of customer data — and identifying the risks that exist at every stage. Attacks may vary, but the most effective mitigation strategies are often very similar, using real-time analytics to maximize security and minimize disruption to the business. In fact, it is imperative that firms look for end-to-end anti-fraud solutions, to ensure that no gaps have been left or vulnerabilities overlooked.

Here are a few key components of the best end-to-end solutions:

- **Identity management and credentialing** confirm that users are who they say they are — and that devices can be trusted — throughout the customer journey
- **Adaptive multi-factor authentication (MFA)** ensures that only authorized users can access critical networks, applications and data — and steps up protection when you need it most
- **Risk management systems** tie complex data together through AI based pattern recognition, powering rapid decisions about licit and illicit transactions
- **Technical analytics** flag insecure configurations, malware, cloned devices, remote access tools and other known attacks
- **Secure physical and logical access management** protects you from the inside out, making sure your employees and assets are safe from malicious actors

And here's how these components fit together to protect the customer journey:

New Account Enrollment	User Log-Ins	Transactions & Payments	Interactions & Account Changes
• ID verification • Document verification • Device fingerprinting	• Anti-cloning technology • Cryptographic protection • Risk-based authentication	• Risk Management Solutions (RMS) • Behavioral biometrics • Malware checks and known threat detection	• Workforce MFA • Dual-signing policies

In the following pages, we'll dive deeper into the dynamics of these scams — and the technologies that can stop each in its tracks.

Deep dive into specific problems and solutions

2

Account Opening Fraud

What is it?

Account opening fraud — also called “new account fraud” or “synthetic fraud” — happens when criminals use fabricated identities to submit false applications for real bank accounts, credit cards, loans and other financial services.
Techniques include:

- Counterfeit IDs leverage stolen personally identifiable information (PII)
- Synthetic identities create new fraudulent IDs using a mix of real and fake information from several different sources
- Deepfakes use AI to invent brand new identities, fabricating images and details that are often startlingly realistic

Educational, financial, government, employment and even medical records — along with social media — are all sources of information for new account fraudsters, who ultimately seek to abuse promotions and instant loans or facilitate the transfer of other ill-gotten gains.

How can I prevent it?

The trick to preventing account fraud does not lie in any single technique, but in solutions that combine multiple technologies to target the organization’s unique needs. That’s why preventing account opening fraud requires a layered identity and access strategy that combines verification at onboarding with strong, phishing-resistant authentication throughout the customer lifecycle.
These methods include:

- Biometric validation to match a selfie to a government-issued ID
- Liveness detection to confirm a real, present person rather than a photo, mask or deepfake
- Digital data checks to validate personal information and assess document authenticity across trusted sources

This preserves your fraud education without tying it to a specific SKU.

Strong Authentication After Onboarding
Even when fraudulent accounts slip through, organizations can limit damage by enforcing phishing-resistant authentication. Passwordless, FIDO-based passkeys reduce account takeover risk, eliminate credential reuse and make synthetic identities far harder to monetize.

A Game of Cat and Mouse

A number of global regulations — from Anti-Money Laundering (AML) and Know Your Customer (KYC) to Politically Exposed Persons (PEP) and other sanctions screening — have attempted to address account opening fraud. It’s important to make sure your security provider understands these regulations and can integrate identity verification tools into your broader strategies.

HID

Attacking the Clones

Top anti-cloning technologies spot device clones by:

- Taking advantage of inbuilt hardware security features on users' devices
- Incorporating multiple layers of cryptographic protection into the authentication process
- Making sure that the breach of any one security key does not compromise the others

Device Cloning

What is it?

Device cloning starts when attackers create an unauthorized copy of someone's mobile device. This copy — real or virtual — enables them to impersonate the device's owner, access sensitive data and execute fraudulent transactions.

How can I prevent it?

Incorporate anti-cloning technology into authentication systems to ensure that anyone who is trying to gain access through a cloned device will be stopped.

These solutions can be built as standalone apps or integrated into existing apps to authenticate user devices and protect log-ins and transactions. The most secure anti-cloning techniques take advantage of inbuilt hardware protections by relying on the so-called secure element (SE). The Secure Element is a tamper-resistant microprocessor that's used to store sensitive data, and it's included in almost all modern smartphones. Laptops have a similar module known as the Trusted Platform Module (TPM).

Another way to thwart would-be cloners: incorporating multiple layers of cryptographic protection into the authentication process. Top solutions structure this in a way that prevents the breach of one security key from compromising any of the others — and thus prevents attackers from being able to impersonate the device.

Credential Attacks

What is it?

Stolen passwords have played a starring role in cybercrime for decades. Over the years, attackers have only grown more sophisticated, using automated tools to trick users into revealing their credentials, then testing them across different platforms. In fact, according to IBM, 2024 saw a 71% year-over-year increase in cyberattacks that used stolen or compromised credentials.

How can I prevent it?

Because credential attacks start with legitimate account information, they can be challenging to prevent. Smart password policies are the first step, supported by **risk-based authentication** solutions that enable organizations to choose when and how to require additional steps.

Institutions might trigger a push notification upon successful password entry or require users to enter a device PIN/password or a biometric marker before accessing their account. Or they might choose to support phishing-resistant passkey authentication and offer a completely passwordless experience. The key is being able to accommodate different journeys based on different types of risk — and provide the right amount of security without slowing users down.

Risk and Reward

Top risk-based authentication technologies stop credential attacks by:

- Enforcing smart password policies
- Stepping up authentication requirements on higher-risk transactions
- Enabling organizations to create customized user journeys that provide the right amount of security without slowing users down

What is SCA?

Secure Customer Authentication, or SCA, is a requirement introduced by Europe's groundbreaking PSD2 directive and echoed by other Open Banking regulations around the world. It's a type of MFA that requires users to provide two or more specific types of identification when they transact online:

- **Knowledge** — Something they know, like a PIN or a password
- **Possession** — Something they have, like a card or a key fob
- **Inherence** — Something they are, like biometrics

Brute-Force Attacks

What is it?

Brute-force attacks use trial-and-error to deduce log-in info and encryption keys. It's simple — and surprisingly effective. In fact, automated tools can now generate and enter millions of passwords within seconds until they find the right one. (Cracking a six-character password that mixes numbers with both upper- and lower-case letters takes a mere six hours, for example.)

Research suggests that brute force was responsible for more than 20% of 2024's attacks on web applications, and a substantially higher proportion of attacks on cloud service providers like Microsoft Azure.

How can I prevent it?

A number of authentication protections can prevent brute-force attacks, from solutions that monitor and limit the number of unusual IP addresses to CAPTCHAs that distinguish between bots and authentic users. Complement these protections with **Strong customer authentication (SCA)** — a type of MFA specifically designed for brute-force attacks — to prevent cracked passwords from giving attackers immediate access to user accounts.

Push notifications, for example, offer a smooth user experience without compromising on security, while passkeys offer a completely passwordless (and phishing-resistant) journey. The most robust solutions enable you to customize settings according to your specific needs and policies, using techniques that include:

- Delay locks set off an escalating series of delays when users enter the wrong credentials, before they can try again
- Counter locks render passwords invalid after a certain number of unsuccessful attempts
- Silent locks give users no feedback when they enter the wrong credentials; they simply lock people out of the system

HID

Account Takeover Fraud

What is it?

Account takeover fraud occurs when malicious actors gain access to a user's account — whether through a breached password or a brute-force attack — and execute unauthorized transactions. Consequences to the victim are often quite severe, ranging from financial loss to outright identity theft. Malware attacks, remote access software and social engineering scams can also lead to account takeover fraud.

How can I prevent it?

Since causes vary, preventing account takeover fraud requires a multi-layered strategy. Strong customer authentication (SCA) provides a critical first defense, preventing breached credentials from giving attackers an automatic pass into users' accounts. Push authentication notifications, which use cryptographic techniques to link a device to its owner's identity, are especially effective, because they make it impossible for attackers to impersonate someone without physical access to their phone, tablet or laptop.

Robust risk management systems provide many additional tools for fighting account takeover fraud, including:

- Real-time analytics that flag insecure configurations, malware, remote access tools and other non-human activity
- Advanced machine learning algorithms that collect and analyze so-called behavioral biometrics — the way users type or hold their phones, the devices and operating systems they rely on, their IP address and geolocation — to spot anomalous activities
- Transactional risk assessments that enable you to react differently to different situations — and step up authentication requirements when, for instance, transactions are unusually large or initiated at unusual times of day

Some systems include just one or two of these tools, but it's worth seeking out a solution that can deliver all three — especially because it will help you address other types of fraud, as well. (We'll cover that in the next few pages.)

Layering Takes the Cake

Security professionals talk a lot about the importance of a multi-layered strategy, in which different technologies protect against different types of threats — and each has a backup to bridge any remaining gaps or flaws. That's because multi-tiered solutions are more than the sum of their parts. Individual layers are critical for addressing specific risks, while together they work to streamline performance and prevent potential threats from falling through the cracks. Multi-layered solutions also reduce false positives without increasing friction for users.

Phishing, Smishing and Vishing

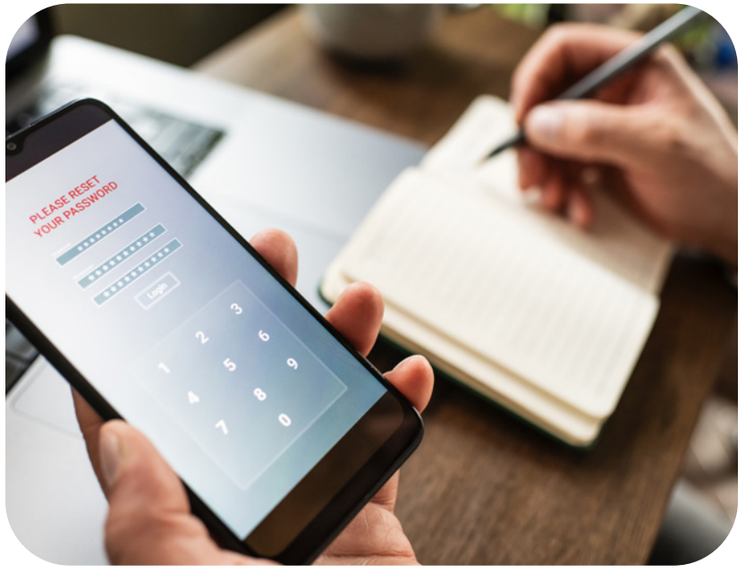
What is it?

Phishing, smishing and vishing are forms of social engineering that trick individuals into divulging sensitive information — whether it's their log-in credentials or an MFA code — to gain access to an account. Variations include:

- Phishing attacks use fraudulent emails to lure users onto websites they believe are legitimate (but are really just designed to trick them into entering their log-in info, and then stealing the data)
- Smishing uses SMS, text messages and phony apps to achieve the same goal
- Vishing relies on phone calls in which scammers (or their AI agents) impersonate government or business officials to con victims into sharing information

How can I prevent it?

The risk management systems we just covered in the previous section shine when account information has been compromised. That's because they combine AI with sophisticated data analysis to provide a real-time view of which log-ins and transactions are — and aren't — normal. The more you know about the way users log in and transact, the faster you can spot anomalous activity … and prevent it from leading to fraud.



Authorized Push Payment Fraud (APP)

What is it?

APP scammers trick victims not into divulging information, but willingly transferring money into a fraudster's account. Some attackers do this by impersonating a trusted individual or authority, while others establish phony charities or fraudulent e-commerce sites. APP fraud is particularly damaging because its victims authorize each payment, making recovery difficult — though in the UK, at least, banks must try, because they're now liable for up to £85,000 worth of damages per incident.

How can I prevent it?

Getting a data-driven view of what's normal and what's not is critical to stopping APP fraud. How, when and where do users typically transact? Does a transaction deviate from those patterns or fit the profile of known threats or attack vectors? Is the customer in an active call while malware is running? Robust risk management systems can deliver this type of analysis in a single, easy-to-implement technology — and identify new threats with relatively little data.

To maximize flexibility and minimize operating expenses, look for a solution that enables you to customize the way you respond to different transactions and types of risk, whether it's an alert or an automatic block. It's also important to find solutions that integrate easily into existing apps and portals, because it gives users the best experience.

Malware

What is it?

Malware is everywhere, but it's especially pernicious for financial service providers due to the many types of malicious software that target mobile banking apps and services. Some programs mimic the interface of a legitimate app or website to capture people's log-in credentials. Others intercept SMS messages and initiate fraudulent transfers — or even let attackers take control of the device. Global mobile banking malware grew 32% in 2023, according to Kaspersky.

How can I prevent it?

Advanced risk management systems extract complex datasets from each application that users have installed on their devices. Then, they compare this information against a reputation database to provide server-side antivirus protections. The best solutions actively look for any signs of attacks, such as Overlay or SMS hijacking, accessibility abuse and more.

SIM Swapping

What is it?

End-users aren't the only targets of today's financial fraudsters. Mobile service providers are an attractive mark, too — especially when fraudsters can convince them to transfer a victim's phone number to a new SIM card that they control. Once this so-called SIM swap is complete, the attacker can access the victim's calls, messages, and, crucially, any two-factor authentication codes that are sent via SMS.

SIM swapping enables fraudsters to impersonate their victims — using their phone numbers to reset passwords, access MFA codes and execute fraudulent transactions. In 2023, the FBI clocked more than 1,000 SIM-swap attacks, concluding that these scams resulted in nearly $50 million in losses.

How can I prevent it?

Advanced risk management systems help organizations spot transactions that originate from new devices and IP addresses. They also recognize when behavioral biometrics deviate from the norm — since it is impossible for fraudsters to move, swipe and type in the same manner as their victims. And they enable banks to customize their response to suspicious transactions, protecting users without disrupting the way they interact with their accounts.

Insider Threats

What is it?

Though many scammers target consumers, financial service employees are vulnerable to the same kind of fraud — especially at organizations that employ insecure authentication methods. Workforce log-in credentials and passwords can be compromised through the techniques we've just described, leaving organizations exposed to dangerous attacks and data breaches.

How can I prevent it?

Multi-factor authentication is critical for protecting access to core banking systems, workstations and applications. The best options can be tailored to your specific use cases and requirements. The key? Choosing a strategy that adds security without compromising productivity and making your employees' lives harder. Options include:

- Phishing-resistant MFA using device-bound passkeys (cards or keys)
- Certificate based authentication using PKI technology (cards or keys)
- OTP hardware tokens
- Biometric authentication

In scenarios with a high risk of corruption, policies like dual-signing with biometric authentication enhance trust by enabling both employees and customers to securely sign transactions.

3

HID Solutions

End-to-End Security, From a Single Source

HID's solutions help banks and financial institutions protect customer accounts without compromising on user experience. Scalable, standards-based technologies cover the entire authentication journey, giving administrators the control to add complexity where it's needed — and remove it where it's not. Solutions include:

- **HID Enterprise Passkey Management (EPM) —** Enable passwordless authentication at scale with secure, device-bound passkeys. EPM simplifies the full lifecycle of FIDO credentials, allowing IT teams to provision, manage and recover passkeys efficiently while reducing helpdesk overhead. With support for remote provisioning, device unlocks and compliance-ready lifecycle management, EPM helps organizations strengthen security without adding friction for users. Learn more >
- **HID Risk Management Solution** — Safeguard banking channels in real-time with a solution that analyzes behavioral and transaction patterns to stop threats. Depending on the level of risk, institutions can opt to grant access, require additional verification or block access attempts to fight fraud without compromising the user experience. Learn more >
- **HID Approve** — Power intuitive, customizable mobile authentication and transaction signing. Options include encrypted push notification, QR codes and secure OTP codes for offline authentication. HID Approve also enables institutions to use device-native biometrics (like facial recognition and fingerprints) to approve transactions. Learn more >
- **HID Crescendo** — Maximize productivity and minimize the risk of insider threats with flexible workforce authenticators that are phishing resistant and instantly compatible with critical enterprise resources and applications. Supporting a broad array of protocols, technical specifications, and regulatory frameworks and certifications — including FIDO2 — Crescendo cards and keys enable you to tailor an MFA framework that aligns with your unique use cases, security requirements, business needs and compliance mandates.

  Learn more about Crescendo Cards >
  Learn more about Crescendo Keys >
- **DigitalPersona** — Protect access to critical banking infrastructure with an MFA solution that supports the industry's widest range of methods, from fingerprint and facial scans to building access cards and FIDO and PKI credentials. Pre-integrated with platforms like Temenos, DigitalPersona enables users to quickly and securely authenticate their identities — from anywhere. Learn more >

4

HID Advisory Services

Fraud Advisory and Mitigation Services

HID complements our award-winning authentication solution offerings with an experienced Fraud Advisory and Mitigation Services team. This dedicated group of cybersecurity analysts, engineers and advisors provides ongoing support and best practices, including:

- Proactive analysis, alerts and guidance on preventing threats
- Purpose-built tools that address specific customer needs
- Automatic tools to identify and take down phishing sites
- A continually updated database of threats
- An on-call security consultancy

Learn more about these services >

Block Fraud, Not Your Customers

Financial fraud is widespread, and it's hard to overstate just how damaging it is. Security is one of consumers' top concerns, with 69% prioritizing fraud protection when selecting a financial institution. Yet 76% also demand real-time access to financial services — forcing institutions to balance innovation with security as they set strategies and design and launch new products.

HID gives organizations the tools they need to strike that balance, delivering scalable identity and authentication solutions that stop fraud without blocking legitimate transactions. By covering the full consumer authentication journey under one vendor, we simplify deployment and integration, providing a seamless experience for banks and customers alike.

Is Security Slowing You Down?

- Explore our fraud prevention solutions >
- Get a fraud prevention demo >
- Speak to a banking security expert >
- Explore success stories from our customers >

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +353 91 506 900
Asia Pacific: +852 3160 9800
Latin America: +52 55 9171-1108

For more global phone numbers click here

2026-01-27-iams-fraud-prevention-handbook-2026-eb-en
PLT-08281

Part of ASSA ABLOY