Daon

# Winning the Fraud Prevention War

a guide for financial institutions

# Winning the Fraud Prevention War

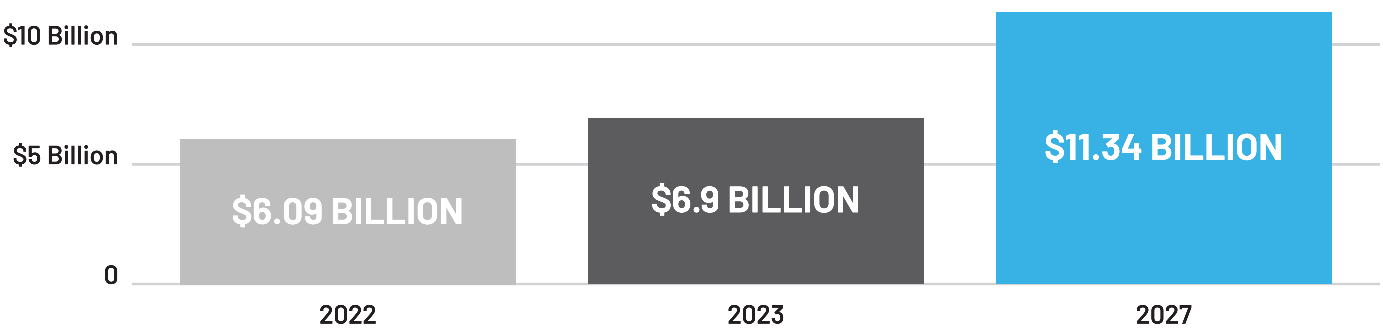
EBV1-1023 ©2023 Daon, Inc. All rights reserved.

# Winning the Fraud Prevention War

The financial sector is undergoing a profound transformation in this increasingly digital age. BankRate's 2023 Digital Banking Trends report found that consumers using mobile banking as their primary method of account access increased from 15.1% of consumers in 2017 to 43.5% in 2021. In today's online landscape, financial transactions occur at the tap of a screen, and ensuring the authenticity of identities and safeguarding sensitive information has become paramount.

Identity theft, fraud, and cyberattacks are more than buzzwords – they're real, costly threats targeting financial institutions and their customer base. Today's financial leaders should turn to identity proofing and authentication solutions to mount a robust defense against fraudsters and to futureproof their organization's security for whatever comes next. Establishing and maintaining trust in a banking institution is pivotal to its reputation, success, and customer satisfaction. Customers must possess a sense of ease and confidence that their identity and, as an extension, their assets, are consistently safeguarded and out of harm's way.

GLOBAL DIGITAL BANKING PLATFORM MARKET GROWTH & EXPECTATIONS



(Global News Wire)

With the right digital identity partner, financial firms can use identity and access management solutions, such as identity proofing and authentication, to fortify their operations and customer relationships.

# Winning the Fraud Prevention War

## Shifting Threats in Fraud and Security

The digital era has brought about an alarming rise in identity theft, fraud, and cyberattacks targeting financial institutions. Statista reports that, in 2022, the U.S. ranked second worldwide for the number of identity theft cases with approximately 13.5 million adult victims.

The most important thing a financial company can provide to a customer is confidence that their identity and assets are protected. A security breach breaks that trust and tarnishes brand reputation. It can be a tricky balance: making account access secure enough to deter fraudsters while making it convenient for customers is a constant challenge for banks in a highly competitive digital market.

In the first half of 2022, U.K. Finance reported just under **30,000 incidents of fraud** in remote banking. The total cost of these incidents was **£85 million**.

Australians reported **$24.6 million in losses to phishing scams in 2022, a 469% increase from 2021.**

ACCC report

Financial institutions must prioritize staying ahead of the fraud curve, especially as today's bad actors employ innovative, ever-evolving methods – like deepfakes and social engineering tactics, such as phishing – to bypass traditional authentication systems. These attacks result in substantial financial losses, erode an organization's reputation, and threaten customer trust in financial institutions.

### Social Engineering

Social engineering is a type of cyberattack where bad actors attempt to retrieve sensitive information by manipulating people into providing personal data, account credentials, or access to networks or systems. The Financial Services Quarterly Threat Landscape Q1 2022 assessment from ZeroFox reported that social engineering has been identified as one of the most frequently reported cyberattack intrusion tactics used by fraudsters targeting the financial sector in Q1 2022.

Phishing is one of the most common social engineering tactics, with the U.S. reporting a staggering 500 million phishing attacks in 2022 – more than twice the number of attacks in 2021, according to the FBI Internet Crimes Report. The Australia Cyber Security Centre recorded over 74,500 incidents in 2022, a 13% increase from the previous year. This rise in incidence isn't unexpected considering that phishing is among the easiest scams for individuals to fall for.

Unsurprisingly, the banking industry is one of the top targets of phishing attacks. Fraudsters pose as financial institutions and send fraudulent emails or messages requesting financial information, like passwords or credit card numbers. Scammers then use the personal data obtained for unauthorized transactions like credit card fraud or identity theft.

# Winning the Fraud Prevention War

And while there are safety protocols built into both internal and consumer-facing banking websites and apps, it is often the human element that fails to detect the scam, resulting in thefts large and small (hence the term "social" engineering). Modern identity proofing and authentication technology is the key to more thoughtful and secure digital banking.

**Deepfakes**

The primary function of identity proofing and authentication is to definitively determine that a person is who they say they are – but what if their voice, appearance, and mannerisms are fabricated? Synthetic identity and deepfake technology have made that possibility a reality. When listening to audio or watching video, one can no longer assume that the person they are hearing or seeing is, in fact, the person they perceive them to be.

Deepfakes are manipulated content – like videos, audio, photos, and text – created using artificial intelligence (AI). Deepfakes are nearly impossible to differentiate from authentic media. While there are legitimate uses for deepfakes, they can also put the financial sector at risk for exploitation and fraud and pose a significant threat to authentication technologies, including facial and voice recognition.

The various scenarios are frightening, from reputational damage due to public-facing security breaches to financial loss from individual-level fraud. Deepfakes can be used for social engineering fraud to steal passwords and personal identity information, to fool biometric authentication that lacks liveness detection or other presentation attack defenses, and more. The threats are exponentially increasing, just as generative AI's growth is.

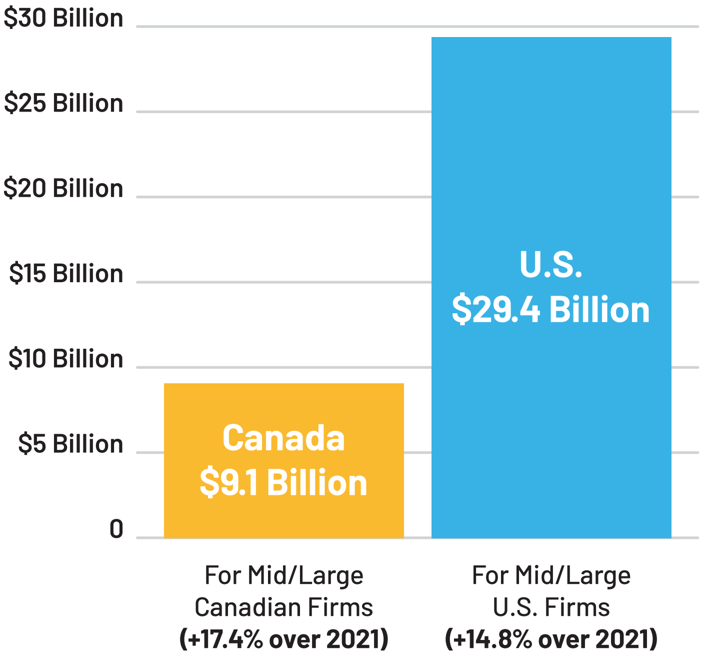
What is certain is that the influx of deepfakes has significantly eroded human defenses against fraud. Banks can no longer count on traditional detection methods, often relying on the discernment of the call center agents to flag manipulated content. Deepfake sophistication has evolved beyond the realm of human detection – and technology must step in as the solution.

**2 out of 3 cyber security professionals** saw malicious deepfakes used as part of a strike against businesses in 2022, a **13% increase** from the previous year, with email as the top delivery method.

(VMWare, "Global Incident Response Threat Report," August 2022)

# Winning the Fraud Prevention War

PROJECTED TOTAL COST OF FINANCIAL CRIME COMPLIANCE ACROSS NORTH AMERICAN FINANCIAL FIRMS (COST IN BILLIONS)



Forrester

## Navigating a Complex Regulatory Landscape

Staying up to date with the legal requirements for all international entities is a demanding task, and organizations that get it wrong could face significant consequences – especially when it comes to global expansion. Financial institutions operate within a complex web of regulatory requirements such as Know Your Customer (KYC), Anti-Money Laundering (AML), and General Data Protection Regulation (GDPR). Guidelines vary from country to country and constantly change, adding to the compliance burden.

Direct financial loss is only one of the costs a business can incur if it falls victim to identity fraud. Depending on the size of the breach, there could also be fines and other governmental levies. And the cost of fraud is only magnified when considering the harm it does to customer relationships.

The Javelin 2022 Identity Fraud Study reported that the average financial loss per identity fraud scam victim was $1,029. That doesn't consider the potential impact on a consumer's credit or the hours spent trying to set things right after their identity is compromised. The impacted customer will likely share their experience with friends, family, social media, and beyond. If a brand doesn't prioritize identity safety and data protection, it can lose current customers and drive away new ones.

KYC, customer due diligence, and transaction monitoring are increasingly intricate, specialized, and time-intensive. This complexity is partially due to the continuous evolution of transaction methods. Now more than ever, financial compliance teams must adopt the advanced biometrics and document verification technologies inherent in identity proofing and authentication solutions to aid in identifying suspicious users and patterns, protecting customer data, and enhancing onboarding and transaction procedures.

# Winning the Fraud Prevention War

## Growing Dispersal of the Customer Base

Customers have been turning to digital channels and away from traditional brick-and-mortar financial establishments for years. Galileo found that 65% of consumers use traditional banks for their primary bank accounts, while JD Power reports that 27% primarily use online banks. However, of the 65% primarily using traditional banks, 77% said they keep some of their funds elsewhere. This dispersal of the customer base presents challenges in providing secure and convenient access to financial services.

Additionally, the shift from in-person to virtual interactions makes treating customers as individuals and considering their unique needs crucial. Customers desire to feel known by their financial institutions and to access their accounts no matter where they are or what channel they use.

Whether customers interact with a brand through social media, on a website, or by email, they have come to expect a personalized experience that makes them feel valued and prioritized. In one study by McKinsey & Company, 71% of consumers said they expect companies to deliver personalized interactions – and 76% get frustrated when this doesn't happen. The personalization that digital banking channels allow is a key part of retaining digital customers and maintaining a positive user experience. Financial institutions face a tricky challenge as customers venture further into the digital wilderness. How can they connect with customers everywhere, on every device, while keeping things secure and user-friendly?

### TOP DIGITAL BANKING USERS BY COUNTRY:

Statista

| UNITED STATES | BRAZIL | UNITED KINGDOM | FRANCE | MEXICO |
|---|---|---|---|---|
| 225.4 MILLION | 72.8 MILLION | 44.2 MILLION | 34.5 MILLION | 44.2 MILLION |

# Winning the Fraud Prevention War

## Balancing Security and Convenience for End Users

It's a common scenario: a customer forgets their password, has to answer security questions, and waits for an email verification code, only to be granted account access minutes later. Traditional authentication methods can be like a maze with no exit, often leaving customers frustrated and with poor user experiences.

Resetting a password may seem insignificant, but it costs organizations time and resources. A Bloomberg article states that between 20-50% of all IT help desk calls are for password resets and range from two to 30 minutes to fix. Forrester Research states that a single password reset's average help desk labor cost is about $70.

The real challenge for financial service providers is balancing tight security with seamless user experience (UX). Stricter verification processes risk alienating users, and lenient ones jeopardize security. Banks must deliver frictionless customer experiences to a demanding client base through all channels: mobile, web, call center, and even in-person.

## The Solution: Identity Proofing and Authentication

Financial services providers sell peace of mind. Their customers believe their monetary assets are safe because of factors like an organization's brand reputation, strict industry regulations, and government assurances, such as FDIC. When a customer experiences advanced security measures during their transaction, trust is established. When those measures cause unnecessary friction, however, customer engagement is damaged. Banks must prepare to battle the changing fraud landscape with futureproof technology that provides best-in-class security and low-friction UX.

**Here are some ways to futureproof your organization against fraud:**

- Conduct standards-based implementations that follow industry data security and privacy best practices, ensuring to only retain and properly store relevant and necessary data.
- Expect constant change and use adaptable identity and access management solutions that simplify adding, updating, and improving features with little disruption.
- Plan for change management and upgrades. A hosted or SaaS solution lets a third-party handle maintenance, upgrades, and improvements.
- Track operational and fraud metrics to understand customer success rates, fraud rates, and costs, and to measure the effectiveness of security solutions.

Banks can build trust in two ways: by keeping customer data safe and by staying compliant with industry regulations. The proof of identity a customer must provide to open an account (identification), how that identity is verified during onboarding (proofing/verification), and the sophistication of the credentials a customer must present for future account access (authentication) all determine an organization's balance between security, compliance, and user experience.

# Winning the Fraud Prevention War

## Identity Proofing for Compliance

With customers routinely creating banking accounts online, financial organizations must be able to confirm that an identity truly exists and belongs to the same person seeking to open or access an account. Digital identity proofing is the process that allows customers to prove their authenticity to an organization. At the most basic level, the customer provides identification (a driver's license or passport) when they register or open an account, and the bank verifies their identity against any relevant third-party and government databases before granting them access.

The fastest, most accurate version of digital identity proofing uses proprietary algorithms, artificial intelligence (AI), and machine learning for instant, accurate document verification and presentation attack detection.

**Digital identity proofing and verification steps:**

- **Step 1** – The customer confirms their consent to have their biometric information captured for verification.
- **Step 2** – The customer snaps photos of the front and back of their identity document, which are instantly subjected to anti-fraud checks.
- **Step 3** – The customer takes a selfie that is checked for liveness via AI-powered algorithms and matched to the image from the identity document.

Identity proofing plays a pivotal role in regulations compliance. More than 90 countries have strict rules mandating that businesses verify customer identities and keep identity records. Designed to reduce online fraud, identity theft, and other cybercrimes, these regulations, such as GDPR and KYC, determine how data are collected, protected, and monitored. Identity proofing helps banks comply with these regulations, thus avoiding censure and fines.

Using digital identity proofing technology to understand, measure, and manage what is happening in real-time is essential to compliance efforts. The ability to differentiate between legitimate and fake identities is crucial to enhancing operational efficiency, reducing compliance expenses, and effectively navigating the landscape of new rules and sanctions.

But the value of accurate identity verification also extends far beyond compliance: it aids in building a trustworthy customer base and mitigates the risk of fraudulent activities.

### GPG 45 | 5 STEPS OF IDENTITY CHECKING

1. Get evidence of the claimed identity
2. Check that the evidence is genuine or valid
3. Check if the claimed identity has existed over time
4. Check if the claimed identity has a high risk of identity fraud
5. Check that the identity belongs to the person who's claiming it

GPG45

# Winning the Fraud Prevention War

## Identity Authentication

In a digital world fraught with scammers and schemes, it's more important than ever for financial organizations to know, without a doubt, that the person accessing an account is who they claim to be. Authentication is the key security step between someone presenting credentials they've previously established and being granted access to their account or data. It can also take place without identity proofing, like when a user is asked to provide step-up authentication for a financial transaction, for example.

Authentication is where the tension between securing accounts against identity fraud and providing easy customer access plays out.

ONE IN FIVE EUROPEANS SUFFERED FROM IDENTITY THEFT BETWEEN 2020 AND 2022.

Finanso

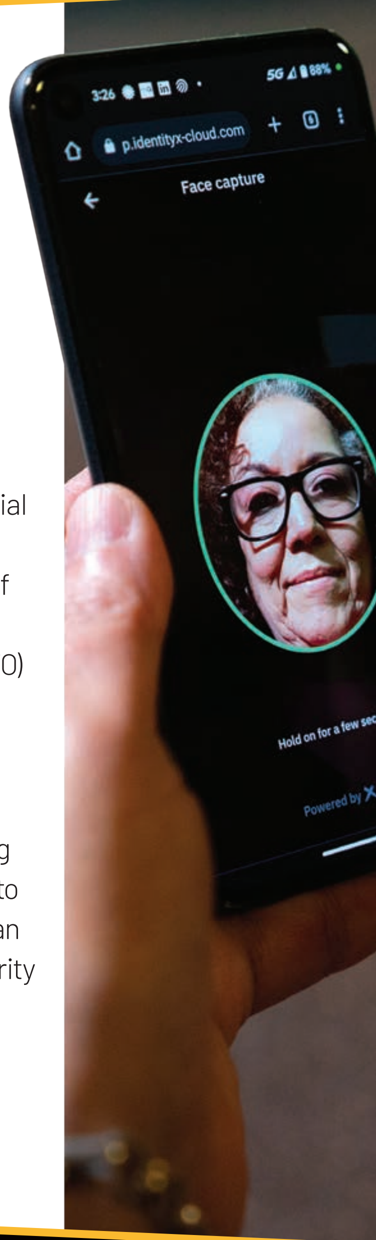
At one time, authentication consisted of confirming that the customer entered the correct username and password to gain account access. While easy to enter, passwords are not secure and are a significant cause of customer frustration. People forget them, lose them, and are forced to jump through hoops to reset them. What's more: password recovery is a huge expense to businesses.

A more secure authentication process involves asking the customer to provide a sophisticated identity factor, such as a facial print (face biometric) or a code sent to their phone. Biometrics provides an advantage over passwords because these factors are nearly impossible to steal or replicate.

### Multi-factor Authentication

In 2021, over 22 billion records were exposed in publicly disclosed data breaches. Darktrace found that credential theft, spoofing, and password stuffing attacks in the U.S. retail sector alone accounted for over 170% more of all observed cyber incidents in 2022 than those in 2021. Security.org reported that 60% of account takeover (ATO) victims used the same password as the one used in a compromised account across multiple accounts.

Banks can decrease the likelihood of an ATO by using multi-factor authentication (MFA). With MFA, after entering a password, for example, a customer would be prompted to input a code sent to their phone, or input the code plus scan their fingerprint on their device's reader. MFA boosts security by making it hard for criminals to use stolen passwords alone, as they would also need the customer's phone, fingerprint, or whatever their chosen second factor is.



By combining different identity factors, MFA creates a strong defense against fraud. Commonly used factors include:

- Knowledge-based: a thing the user knows, such as a password or PIN.
- Possession-based: a thing the user has, such as a mobile phone or computer.
- Biometrics-based: who the user is – a biological trait like a fingerprint, face print, or voice print, or a behavioral trait like typing speed, gait, or screen pressure.

### Benefits of MFA

***Increased security***

No authentication factor – even biometrics – is 100% secure. Getting as close to full-coverage protection from fraud as possible requires an additional factor. When layered together, the factors become part of an innovative security system that defends against fraud better than traditional measures. According to the U.S. Cybersecurity & Infrastructure Security Agency (CISA), "Users who enable MFA are significantly less likely to get hacked." If hackers get around one factor, the additional factors reduce the likelihood of their ultimate success.

***Regulatory compliance***

Financial services organizations, and banks specifically, have rules around data protection. Requirements like PSD2 SCA and NIST AAL2 are just two of the many compliance considerations some businesses must keep in mind. Implementing MFA avoids incurring hefty fines for non-compliance as well as the potential damage to reputation and erosion of customer trust straying from these regulations could cause.

***Customer trust***

Customers want their data protected but crave easy access to their accounts. From the moment a customer onboards, an organization that uses MFA shows them that it takes data protection seriously. Yet, because MFA can use factors that run invisibly in the background, a business can also build customer trust without friction, creating a smooth user experience.

When using biometrics as part of MFA, customers and banking organizations can experience the most secure form of authentication available for a modern digital identity management strategy.

### Biometric Authentication

Biometrics are the physical and behavioral characteristics used to verify a person's identity during authentication. Biometric authentication uses secure "templates" of a person's traits (whether a face scan, voice print, or typing speed) that are captured using AI-powered algorithms to authenticate a user's identity before an organization grants them account or transaction access. The biometric template is stored for future authentications and cannot be reverse engineered by fraudsters. So no, no one can "steal" your customer's face!

Some standard biometric factors include fingerprints, face prints, and voice recognition. These factors are more secure than traditional or knowledge-

# Winning the Fraud Prevention War

based methods, like passwords and PINs, as biological characteristics are unique to each individual and cannot be easily replicated, stolen, lost, or forgotten.

As technology continues to advance, biometric authentication is poised to become the primary method of verifying identity and accessing financial services. For slow adopters, this digital transformation creates the threat of being left behind. As fraud increases, financial organizations must turn to biometric authentication to provide the highest level of protection for their customers, employees, and data.

### Benefits of biometric authentication

***Overcome the weaknesses of passwords***

Biometric authentication provides more robust protection against fraud than password-based authentication. Biometric factors can't be lost or shared and don't contain personal information readily available to fraudsters online. Biometrics are also immune to the types of fraud that passwords and other knowledge-based authentication factors are vulnerable to, such as social engineering and man-in-the-middle attacks.

***Increased security against fraudsters***

Unlike widely available personal information that hackers can find online and use to access an account, only a single, unique person can possess or access their own biometric data. Identity proofing and authentication technologies such as AI-powered liveness detection ensure that still images, video captures, or voice recordings (known as presentation attacks) can't be manipulated and substituted for corresponding biometric factors. Biometric templates cannot be reverse engineered, making them low-risk for data breaches.

***Enhanced convenience for customers***

Biometric authentication is simple for customers, only requiring them to, for example, press their fingerprint against a scanner or take a selfie. There's nothing to remember and no other items necessary for the user to have in their possession. People are already familiar with biometrics, increasing its perceived convenience, security, and adoption rate. Financial services organizations that use biometrics can show their commitment to being attuned to what modern consumers want.

*********

**39%** of consumers use the same password for every service

**79%** of Americans share their passwords with people outside their homes

**59%** of U.S. adults have incorporated a name or birthdate into their password for an online account.

2020 Google study

# Winning the Fraud Prevention War

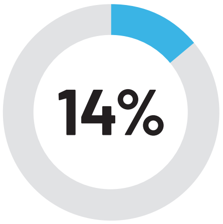
***Reduced costs***

Businesses spend an incredible amount of time and money dealing with password resets annually. Gartner estimates that 40% of all support calls are for password resets, and employees lose 11 hours per year just handling these resets. Forrester estimates that each individual password reset costs $70.

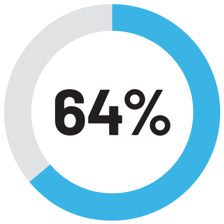
Biometrics eliminates any need for password resets, because who you are can't be lost, stolen, or replicated.

Beyond the direct financial costs, there is also the question of customer churn. When customers are required to continually go through steps that they find frustrating in order to do business with an organization, then end result, more often than not, is that they go somewhere that doesn't require those steps.

A study by Google showed a shocking percentage of failure authenticating with passwords. In the same study, almost 5 times as many people succeeded using biometrics.

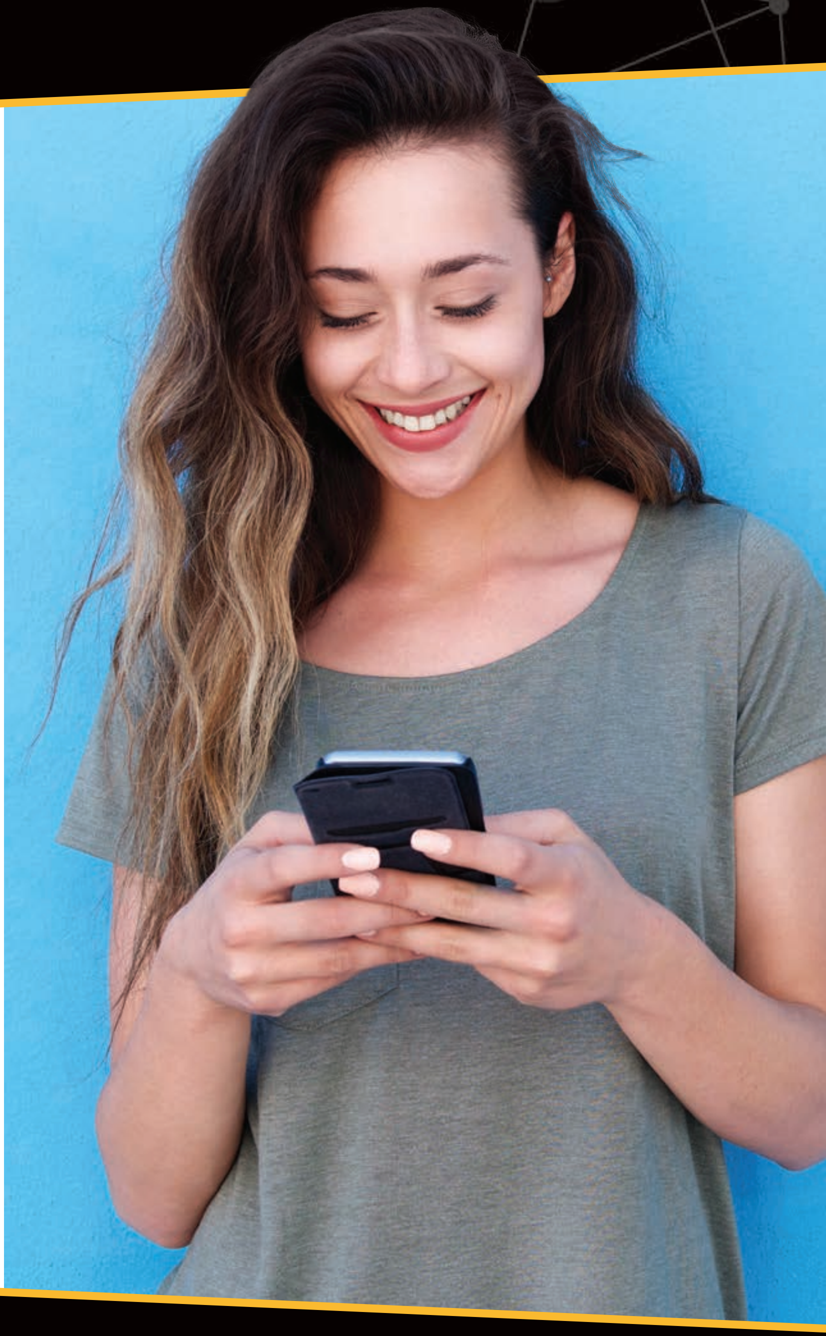


**Success authenticating with passwords**



**Success authenticating with Google's biometric passkeys**

These numbers directly correlate to customer satisfaction and, in turn, customer retention.

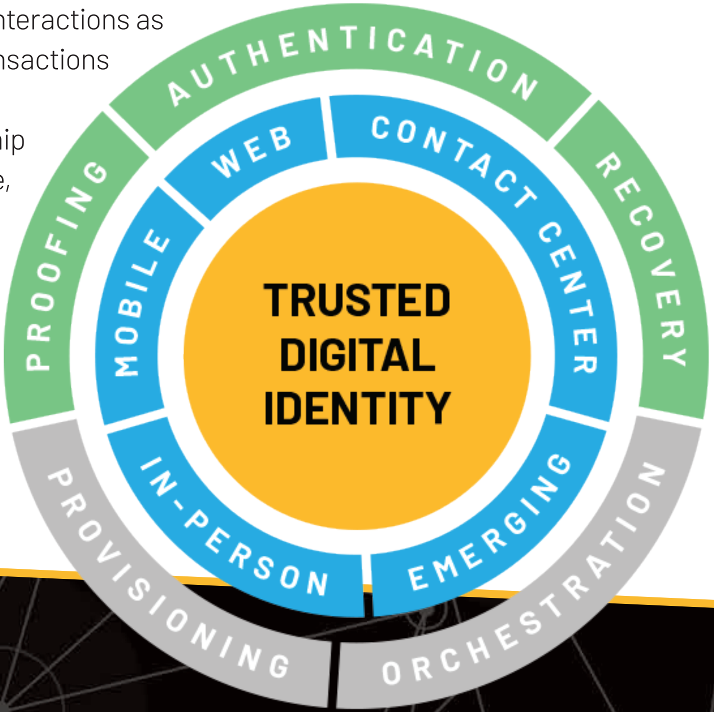


# Winning the Fraud Prevention War

## Identity Continuity

Identity Continuity centralizes, simplifies, and enhances the steps in identity proofing and authentication. Developed by Daon, Identity Continuity seamlessly merges identity proofing and verification, authentication, and account recovery across all channels. The key is that a customer onboards once with a proven identity, and then uses that singular identity to authenticate at every point of entry, from anywhere, through any channel. This is possible because the functionality of all three solutions exists on a single, AI-powered platform.

By streamlining identity management, Identity Continuity builds lifelong trust throughout a customer's digital identity journey. It's a shift from treating customer interactions as separate, siloed transactions to recognizing the customer relationship as the single, unique, personalized, and consistent digital identity experience it should be.



### Benefits of Identity Continuity

By taking a new approach to familiar processes, Identity Continuity offers banks the opportunity to improve customer satisfaction and security while reducing costs – all without any heavy lifting.

Each customer wishing to access an account uses a single identity, established once and seamlessly authenticated going forward. The customer's identity is accessible through any channel – web, apps, contact centers, kiosks, in-person – any time, with low friction and seamless movement.

Identity Continuity gives financial institutions greater control and visibility into their customers' identity journeys and brand interactions. By adopting a single, central view of the customer, a bank can determine the unique behaviors of that person to serve them better, improve their brand's reputation, lower abandonment rates, and gain valuable insights to customize services based on customer actions and needs.

Together, these benefits result in improved customer experiences.

By leveraging biometrics and AI-driven technologies during the identity proofing and authentication process, Identity Continuity reduces the potential for fraud from the moment a customer opens an account. Through establishing a single identity, Identity Continuity closes gaps and discrepancies between customer accounts that can provide additional points of entry for criminals and increase fraud, such as through ATOs and synthetic fraud attacks.

With Identity Continuity, fraud can be a thing of the past.

# Winning the Fraud Prevention War

## The Daon Difference

Daon is one of the top digital identity companies and an industry leader in next-gen identity proofing and biometric multi-factor authentication. Since 2000, our engineers and scientists have patented and brought to market more biometric identity verification systems and technologies than any team, anywhere. Serving over 150 global financial institutions, we stand as a beacon of trust for some of the world's most iconic brands.

app.identityx-cloud.com
Face capture
Make sure that your face is in focus and that the photo is clear before uploading
Retake The Photo
Continue
Powered by Daon

### Minimize Risks, Minimize Costs

According to the latest True Cost of Compliance report from Forrester, UK financial services organizations spend £34.2 billion yearly on financial crime compliance (FCC). While banks and fintechs invest billions in technology to automate processes, siloed and legacy methods stand in the way of efficiency gains. Daon specializes in solutions for the financial sector that address the challenges of balancing security and convenience for customer identity proofing and authentication. Our technologies ensure that the right person connects to a financial company – the first time and every time after that.

At Daon, we've spent over 20 years developing our platforms to create the most seamless and secure solutions for a customer's identity lifecycle. We call this all-encompassing services delivery approach Identity Continuity, and it's the foundation of our hosted and SaaS solutions, both of which support our full suite of identity proofing and authentication products across all channels.

# Winning the Fraud Prevention War

## TrustX™

Our cloud-native, SaaS Identity Continuity platform, TrustX, transforms the customer's digital identity journey. No development team is required: our no-code, drag-and-drop setup and configurations allow financial institutions to customize workflows themselves, eliminating high costs and lengthy implementation cycles. TrustX stands apart with its speed, simplicity, and orchestration capabilities, revolutionizing how financial institutions approach identity proofing and authentication.

## IdentityX®

IdentityX is Daon's 5th generation hosted identity management platform that supports all of our identity proofing and authentication applications across multiple channels. Effortlessly navigate compliance, mitigate fraud with 3rd party identity checks, and KYC easier and more seamlessly than ever before – even when you augment existing infrastructure. IdentityX is specifically designed to operate both on-premise or in a private cloud to support the internal requirements or external regulations that many financial services organizations must consider.

## xProof™

Virtually eliminate ID fraud during onboarding with xProof. Our solution's identity proofing and verification technology leverages biometrics to minimize friction and maximize compliance. Powered by proprietary AI algorithms for accurate document verification, and featuring industry-leading presentation attack detection, xProof gives you everything you need to securely onboard new financial services customers anytime, from anywhere.

## xAuth™

Virtually eliminate ID fraud during onboarding with xProof. Our solution's identity proofing and verification technology leverages biometrics to minimize friction and maximize compliance. Powered by proprietary AI algorithms for accurate document verification, and featuring industry-leading presentation attack detection, xProof gives you everything you need to securely onboard new financial services customers anytime, from anywhere.

## xFace

Our biometric facial authentication delivers maximum security, meets the most stringent regulatory requirements, and provides step-up authentication for high-value transactions that surpasses on-device biometrics. Built on proprietary Daon algorithms, driven by AI technology, and secured against presentation attacks, xFace provides optimum protection from identity fraud while keeping your finance customers happy with the ease of use inherent in face biometrics.

## xVoice™

Seamlessly harness the power of voice to authenticate any customer, anywhere – in seconds. Keep fraudsters out with advanced anti-spoofing technology powered by AI and machine-learning algorithms trained to detect synthetic speech and voice replay. xVoice was built to integrate seamlessly with existing IVR, offers passive registration and authentication for little to no customer friction, and supports MFA for high-value financial transactions.

# Winning the Fraud Prevention War

## Win the War Against Fraud

In a rapidly evolving digital landscape, identity proofing and authentication have become cornerstones of the financial sector's success. Financial services organizations must recognize the urgency of adopting innovative solutions to counter the growing threats of identity theft, fraud, and cyberattacks. Banks can protect their customers and build lasting trust by prioritizing security, compliance, and UX – embodied by Identity Continuity, Daon's holistic approach to customer identity and access management. As financial entities forge ahead in a digital-first world, the integration of effective identity proofing and authentication processes will be critical to their success.

VISIT US ONLINE TO LEARN MORE ABOUT DAON'S POWERFUL DIGITAL IDENTITY SOLUTIONS.

daon.com/solutions

Daon®

The
**Digital Identity Trust**
Company