TRUSTED IDENTITY

From Start to Finish

How Liveness Detection and Face Biometrics Make Data Breaches Irrelevant

A FINDBIOMETRICS WHITE PAPER

SPONSORED BY JUMIO facetec

Part One: We Need to Break the Data Breach Cycle

Data breaches are a major threat to a safe digital future.

The data breaches peppering the mainstream media news are an indictment of the modern cybersecurity landscape. Caused by a number of factors, including human error, unpatched systems, malware infections, insider threats, stolen devices and, of course, poor password hygiene, data breaches are responsible for eroding trust in companies of all sizes damaging their brand image and budgets. From a timeline spanning as far back as 2013, when the first of the landmark Yahoo data breaches occurred, through the end of 2019, which saw the breaches of Quest Diagnostics, Capital One and Lenovo among many others, one could easily characterize the 2010s as the **"Decade of the Data Breach."**

The "Decade of the Data Breach" affected us all. Regardless of whether you were among the billions of users whose Personally Identifiable Information (PII) leaked in the Yahoo, Uber, TimeHop, Equifax, or OPM breaches, your personal security and privacy diminished as a result of inadequate data and identity management practices. Every data breach leaks PII, and that PII — names, emails, phone numbers, Social Security numbers, addresses, passwords, transaction histories and credit info — is sold in large batches on the dark web. Those batches are, in turn, used by fraudsters to conduct phishing campaigns, social engineering scams, and targeted brute force sieges, cracking the shells of more databases and leaking *even more* PII. And the cycle continues, each breach making the next more feasible while dramatically eroding trust in the brands responsible for protecting user data in the first place.

The problem is with our keys. Because of the rise of the dark web, identity theft, and account takeovers, enterprises can no longer trust that the person creating an online account (or logging into an existing one) is who they claim to be. Knowl-

THE DAMAGE IN DOLLARS

According to IBM Security's *2019 Cost of a Data Breach Report*, an average-sized data breach (25,575 records) costs a company $3.92 million. And that's just to identify and contain it. Breaches carry with them additional costs in severe damage to a company's brand reputation, lost customer trust and class action lawsuits. Here are a few settlements from some of the more high-profile breaches of the past few years:

Yahoo: $117.5 million

Equifax: $700 million

Uber: $148 million

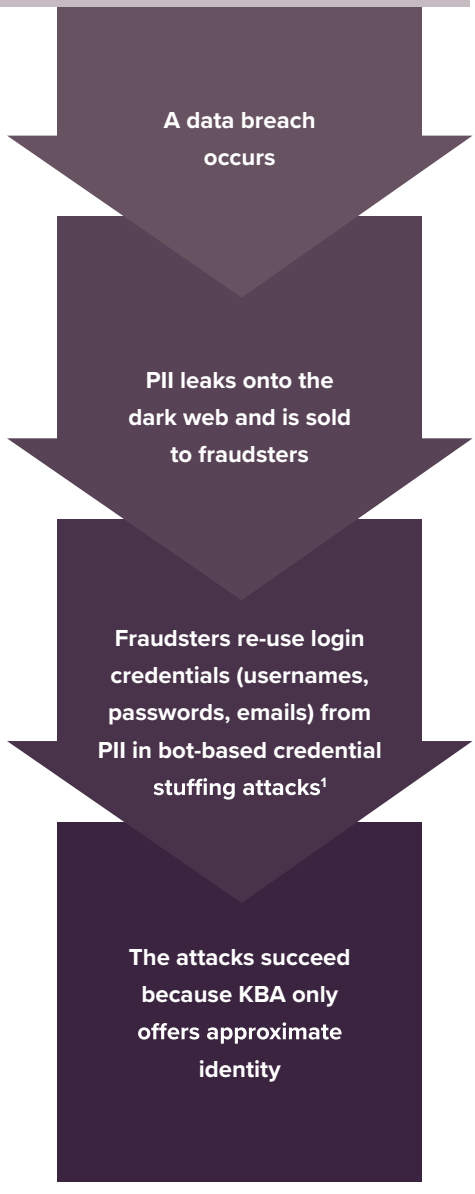
edge-based authentication (KBA), like passwords, PINs and security questions, historically forms the foundation of digital security. In some cases, this is bolstered by multi-factor authentication, like SMS-based one-time passwords (OTP), authenticator apps based on smartphone push notifications, and other device-based security. But clearly, the status quo isn't working, and we know why: KBA and device-based security factors only offer *approximations* of identity.

HOW A DATA BREACH MAKES USERS VULNERABLE TO ACCOUNT TAKEOVER AND FRAUD

Knowledge-based authentication is just that: something you know. It's information, and as the old maxim goes, information wants to be free. Something you know is only one step away from something someone else knows. KBA can be guessed, stolen, shared, cracked with software, or bought online. And once someone else knows a password or PIN, there is no telling whether a transaction is being conducted by an authorized user or an impostor.

Device-based authentication, often used to bolster KBA, does offer a higher grade of security, but still only delivers an approximation of identity. Even biometric authentication conducted on-device only truly proves that the user conducting the transaction is using a verified trusted device, not that they are who they claim to be. Lower grades of device authentication are susceptible to social engineering (in which users are tricked into divulging OTPs in real time), spoofing (in which a virtual copy of a device is used to fool a security system), remote access trojans (in which an authorized device is hijacked by malware and used to conduct transactions), and many other constantly evolving cybercrime techniques.

Data breaches are not going away, so we need to shift from approximate identity to trusted identity. That means proving a person is who they claim to be from their very first brand touchpoint using government-issued ID and biometrics. It means authenticating every subsequent transaction solely with an irrefutable human element, instead of a trusted device or login credential. And it means ensuring human liveness — rather than an impersonation or "spoof" — is part of every point of interaction, maintaining the integrity of an identity-based security system from start to finish. We need a weapons-grade approach to authentication and identity proofing, as long as it isn't more painful or time-consuming.



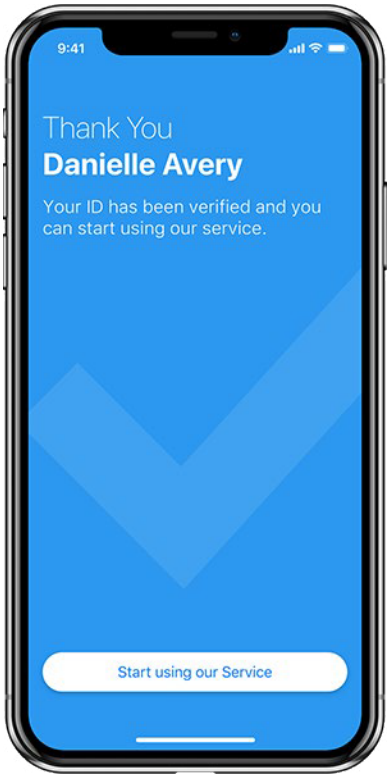
[1] PerimeterX research reports credential stuffing attacks have an 8 percent success rate.

In September 2019, the Identity Theft Resource Center marked a bleak milestone. Since it started cataloging the events in 2005, it has logged 10,000 publicly notified data breaches. Year after year, breaches and record exposures have risen, along with their costs — including penalties associated with privacy-centric government regulations. Every user on a system is a potential vector for a breach. But not by choice. Exhausted by the burden of managing dozens of complicated, high-maintenance passwords and time-consuming second-factor authentication, the average user wants an easier time at the login screen with the assurance they're not at risk of being sucked up into the next explosive data breach headline. No one wants to be a statistic. They want to be a human being protected by high-grade security with an optimal user experience.

Part Two: **Starting with the Human Element**

Anchoring trust puts people back at the core of ID.

We naturally understand identity through human presence, and until now we've had to compromise on this when interacting in digital spaces. The currently accepted methods of online authentication do not guarantee a live human is at the controls – only the device, browser, or a person who knows the password. It's counterintuitive and identity-adjacent. In physical spaces, when we interact with people we trust — be they family members or frequented businesses — we automatically recognize the identity of the person. When you visit your father, he doesn't send you a verification code via text before he can trust it's you, he just identifies you naturally.



MAKING A TRUST IDENTITY ANCHOR – A trust anchor can be accomplished by establishing the authenticity of a government-issued identity document (e.g., a driver's license). From there, you can layer on biometrics and liveness detection to ensure the person providing that credential is physically present. The trust anchor is established at the beginning of the online relationship and carries over into the future for all subsequent authentication events.

1. Take a photo of the front and back of a government-issued ID with a smartphone or webcam
2. Take a selfie to prove the photo ID is yours
3. Perform liveness detection to ensure that the person behind the online account is physically present. NOTE: During the liveness check, biometric data from the physically present user is captured and tethered to the user's digital identity

Liveness detection must take place during the selfie matching and biometric enrollment process and confirms human presence, irrefutably tying the enrolled user's biological identity to his or her digital credential. That's all it takes to anchor a chain of trust.

The foundation of intuitive trusted identity is the onboarding process. During enrollment, it is imperative to identity-proof new customers by anchoring their digital identity to a biometric, such as a face or fingerprint. Government-issued ID represents the top standard for identity verification, and when presented by the rightful user during enrollment it creates a powerful basis for subsequent authentications. This is a trust anchor. It ensures everyone enrolled in a system is exactly who they say they are, and prevents the spawning of duplicate templates, which are a major security concern. One true user gets one secure account. Without the verification of a government-issued ID, a biometric enrollment is security without accountability.

The demands of today's online consumers who want a fast and easy onboarding experience often run counter to the relatively rigorous, full-scale identity proofing required for every user on a system to have a trust anchor. However, commercial solutions exist today which combine ID proofing, corroborating selfies and certified liveness detection, together capable of establishing a reliable trust anchor from any device, be it a smartphone, laptop, or desktop PC. With human presence bolstered by a verified government ID, the biometric enrollment can therefore be trusted as representing a full user identity, rather than an anonymous device owner. In other words: approximate identity can be replaced with true 100-percent-unique digital identity.

A trust anchor — established through a convenient, automated, guided process performed by every end-user — ensures that from the very start, everyone in a system is known, authorized, and empowered with credentials only they can access: their biometrics.

CERTIFIED LIVENESS MAKES CENTRALIZED SAFE — By deleting the liveness data from the server after each session, centralized authentication systems become just as secure as on-device biometric methods like Face ID and FIDO-style authenticators that keep data on the device. In a centralized authentication system, the biometric data does leave the device, but it can't be reused once the liveness data is purged. The result is a biometric authentication system that does not rely on the secrecy of biometric data for security. Instead, it relies on new liveness data being captured from the user each and every time they login. This ensures that even if the server was breached the user can never be impersonated because the stored biometric matching data is not sufficient on its own to facilitate a login.

Part Three:
Checking In, Always

A security system is only as strong as its weakest lock.

Even after proper identity proofing, every subsequent interaction ought to be assured to the same degree. After all, once you open a bank account at a local branch, they don't stop asking for your card, PIN and human presence for transactions. It is necessary that the same high level of assurance used in creating a trust anchor is practiced during every subsequent link of the proverbial chain. One weak link can break the whole thing, sending data adrift.

FACING THE FUTURE OF AUTHENTICATION — Any biometric — fingerprint, face, iris, voice, or even EKG — can be used to onboard and subsequently authenticate users. And while that flexibility of choice is important for accessibility reasons, face biometrics is quickly emerging as the dominant modality thanks to its intuitive, contactless, and web-based experience. It can be used on any connected device with a standard 2D camera that performs with high speed and accuracy, and takes advantage of a deeply familiar cultural gesture: the selfie. With face biometrics powering both identity verification and authentication, you can sign up with a bank remotely and manage your finances from any standard smart device, regardless of its specialized biometric hardware.

Even after proper identity proofing, KBA and SMS-based two-factor authentication still suffer from the same security pitfalls described above. A password attached to a verified identity can still be compromised, as can a second factor token or card. These are the weak links. A biometric remains the strongest and most intuitive choice for subsequent authentications, and it's also the most convenient method. What's more, thanks to consumer grade biometric access features on smartphones — especially Apple's Face ID and the 3D Face Unlock on the new Google Pixel 4 — the average user is becoming increasingly familiar and comfortable with unlocking smartphones with a convenient face-scan.

Aiming to offer the best user experience in addition to making data breaches irrelevant, the ideal end-to-end identity solution is frictionless, contactless, fast, and device-agnostic. Face-based authentication, deployed in a centralized manner, ensures biometric authentication can be implemented at a consistently high quality no matter where a user is or what device they are using.

With a foundation of strong identity proofing, centralized biometric authentication enables an incredible range of use cases, all benefitting from the promise that optimal user experience comes with virtual immunity from data breaches.

USE CASE	USER EXPERIENCE
Making a $10,000 Bank Transfer 	If your banking credentials are compromised, you don't want some bad actor to steal your money. With an established trust anchor and an unbroken chain of biometric authentication, that can't happen. A single biometric scan, supported by certified liveness detection, is all it takes to authorize high-risk transactions.
Logging into an Online Gaming App 	Online and mobile gaming is subject to strict Know Your Customer and Anti-Money Laundering regulations, in addition to age restrictions that vary depending on region. Unimpeachable biometric login supported by a trust anchor ensures KYC and AML compliance while also making it impossible for a minor to access an online gaming platform using an adult's account.
Renting a Car with Your Smartphone 	Paired with NFC and BLE-enabled mobile key technology, renting a car can be easier and provide more accountability than ever. Book a car on your mobile device, and establish a trust anchor with your valid driver's license. Biometric authentication can then be used to unlock your rented vehicle in the lot. No more lines at the check-in desk, no more lengthy sign-up processes. Just get in the car and drive.
Frictionless Hotel Booking 	Establish your trust anchor as you book your hotel online and go straight to your room. Use your mobile device to unlock your hotel door – bypassing the registration lines and hassles normally associated with the check-in process.
Employee Time Management 	In the age of remote work and the gig economy, biometric authentication with an anchored foundation ensures employee and contractor accountability. A user logs into work portals with their irrefutable biometrics via a simple scan, and employers stay protected from time theft and workplace liabilities (rideshare drivers sharing taxi duties, unauthorized persons accessing company accounts).

Part Four:
Not All “Liveness” is Equal

Liveness detection must be robust enough to stop today’s sophisticated fraud.

Biometrics are only a functionally superior replacement for KBA and SMS based second-factor authentication if they are supported by certified liveness detection: independently vetted technology developed to differentiate between a real human biometric and a fraudulent artifact, or “spoof.” In the same way your bank teller can see if you are wearing a mask at the counter in an attempt to impersonate someone else, your biometric authentication should be able to distinguish between your real face and a recorded video, high-definition picture, or digital deepfake. That’s the job of liveness detection.

The evolutionary journey from measuring biometric characteristics for unique matching to irrefutable authentication of a live human being has been long and fruitful, but it has led to a spectrum of biometric “liveness” abilities claims, the lower end of which has proven inadequate against modern fraud techniques. Gesture-based gimmicks, like asking a user to blink or speak a random passcode, add friction to the experience, and are also easily fooled by basic spoofing techniques.

The most robust forms of liveness detection rely on machine learning, AI, and computer vision to examine dozens of miniscule details, from a selfie video such as hair and skin texture, micromovements, and reflections in a user's eye. It is non-invasive and doesn't add friction to the authentication procedure, while guaranteeing integrity for every authentication. And best of all, it can be performed in under two seconds.

With demand for liveness detection being so high, the term itself has become a buzzword and catch-all term for all solutions on the presentation attack detection spectrum. Thankfully, trusted third-party testing has emerged to offer guidance for those looking for the strongest trust chain. Prime among these testers

Best-in-class liveness detection guarantees human presence on every transaction without adding friction to the user experience.

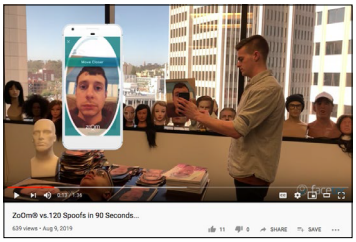
is the NIST/NVLAP-accredited testing lab, iBeta, whose three-tier system stands as the industry benchmark for liveness detection. Each level of iBeta certification (Levels 1, 2, and 3) correspond to the three levels of presentation attack recognized by the biometrics industry (Levels A, B, and C):

- iBeta Level 1 certifies against Level A presentation attacks: short attacks that can be conducted by anyone using readily available materials and equipment like digital images displayed on the phone, or printed out paper images.
- iBeta Level 2 certifies against Level B presentation attacks: sustained efforts conducted by moderately skilled spoofers using prepared materials like masks made of silicon, latex or resin.
- iBeta Level 3 certifies against Level C presentation attacks: ten-day efforts conducted by highly skilled spoofers using specialized equipment like custom made silicone masks or expertly applied theatrical special effects makeup.

With sanctioned third-party testing sorting out the various levels of liveness detection, all of the technological ingredients are available to protect users and businesses in the decade of the data breach. By requiring returning users to capture a selfie and re-establish “liveness,” it's virtually impossible for fraudsters to take over existing accounts. The liveness detection process establishes a liveness baseline, anchoring the ID and allowing the creation of a valid account. It then removes the liveness data – a critical part of the data access "key" – preventing access to the data and rendering the hacking effort worthless.

ZoOm’s CERTIFIED LIVENESS DETECTION – A prime example of liveness detection done right is ZoOm 3D Face Authentication from FaceTec. Thanks to its novel ability to capture 3D facemaps using a standard 2D camera, ZoOm benefits from face data orders of magnitude greater than those of standard 2D face matchers. This extra data enables its liveness detection algorithm to work its magic. Certified by iBeta for Level 1 and Level 2 PAD (passing both assessments with a 100-percent anti-spoofing score), ZoOm isn’t just easy to use, it’s iBeta tested to protect you from today’s most sophisticated biometric hackers.

Watch ZoOm’s liveness detection in action:



Part Five: **The Future of Trust in Our Connected World**

Intuitive trust and reliable security will enable a truly user-friendly future in which data breaches don't empower fraudsters.

If we don't have strong biometric verification and authentication strengthening every online transaction from start to finish, we're in for a whole lot of trouble as new generations of connectivity and mobility emerge. Data breaches are increasing in frequency and scale, accelerating the feedback loop of cyber fraud and successful hacks. Without the trust of ceaselessly victimized end-users, adoption of mobile services will stagger as businesses buckle under the mounting cost of data breach responses.

The only answer is to make data breaches irrelevant to your business and its customers by implementing identity proofing and continual strong authentication, secured by biometrics and liveness detection at every step. The process elegantly locks the bad guys out of user records by creating a singular key based on biological uniqueness and human presence. Liveness data is not part of the stored biometric template and it's deleted after every scan, so every authentication attempt demands a new liveness check. There are two parts to each strong biometric key, and one is only inherent to your own living body.

The scale of change required may sound daunting, but the fact is software-based solutions offering converged identity proofing and strong authentication exist now and can be implemented within just days.

Jumio, a provider of AI-powered identity verification, and 3D face authentication specialist FaceTec, have partnered to make a converged identity proofing/continuous authentication solution that is easy to implement and easier to use. FaceTec's iBeta Level 2 certified liveness detection protects the onboarding and authentication processes from presentation attacks at every step, while Jumio's Identity Verification anchors every user to his or her account. It's centralized, and private by design (ZoOm

TRUE NEXT-GENERATION THINKING – Millennials lead online banking adoption, making up nearly half of the user base, and that means security mustn't come at the cost of convenience. In a 2018 survey, Javelin Research found that as a demographic millennials are the most likely to abandon mobile banking due to poor user experience, with a third of those surveyed reporting they are vocal about their dissatisfaction with their banking institution. The best way to keep millennials banking on mobile is through biometric-based identity verification during onboarding and ongoing user authentication supported by certified liveness detection from the beginning.

deletes crucial liveness data after every authentication). That means that with Jumio and FaceTec:

- Every new account relies on the capture of a trust anchor (e.g., picture of a valid government-issued ID).
- The user provides a corroborating selfie to ensure that the person behind the ID document is the same person pictured on the ID.
- Every new account undergoes certified liveness detection to ensure that the person behind the account is physically present (and not spoofing the process with a deepfake or prerecorded video).
- Every subsequent transaction is authenticated easily and securely with a spoof-proof biometric scan, on any device without the need to enroll again.
- PII is protected by a weapons-grade chain of trust.
- The vicious cycle of PII re-use on the dark web will dwindle, as successful data breaches won't grant attackers access to PII in the first place. Coming up against biometrics and spoof-proof liveness detection, bad actors are left locked out of user records.

Jumio and FaceTec can make data breaches irrelevant to your business, now. To learn how, contact:

Dean Nicolls
Vice President, Global Marketing
Jumio
dean.nicolls@jumio.com

John Wojewidka
VP of Communications
FaceTec
johnw@facetec.com

About Jumio

When identity matters, trust Jumio. Jumio's mission is to make the internet a safer place by protecting the ecosystems of businesses through cutting-edge online identity verification and authentication services that quickly and accurately connect a person's online and real-world identities. Jumio's end-to-end identity verification solutions fight fraud, maintain compliance and onboard good customers faster.

Leveraging advanced technology including augmented intelligence, AI, biometrics, machine learning, certified 3D liveness detection and human review, Jumio helps organizations meet regulatory compliance including KYC, AML CCPA and GDPR and definitively establish the digital identity of their customers. Jumio has verified more than 200 million identities issued by over 200 countries and territories from real-time web and mobile transactions. Jumio's solutions are used by leading companies in the financial services, sharing economy, digital currency, retail, travel and online gaming sectors. Based in Palo Alto, Jumio operates globally with offices in North America, Latin America, Europe and Asia Pacific and has been the recipient of numerous awards for innovation. For more information, please visit www.jumio.com.

About FaceTec

FaceTec's patented, class-leading 3D face authentication software, ZoOm®, anchors digital identities, establishing the chain of trust for mobile and web applications requiring Certified Liveness Detection. Leveraging decades of experience in computer vision, artificial intelligence and advanced biometrics, ZoOm is fast becoming the global standard in onboarding, KYC, and ongoing authentication. Founded in 2013 with offices in San Diego, CA and Summerlin, NV, ZoOm provides strong biometric security for millions of users on six continents for many of the world's leading organizations in IAM/IDV, financial services, mobile payments, border security, connected transportation, blockchain/crypto currency, e-voting, and more.