VERIDIUM
TRUSTED DIGITAL IDENTITY

BIOMETRIC AUTHENTICATION IN FINANCIAL SERVICES

Strong Authentication for
Banking, Trading and Mobile Payments

White Paper

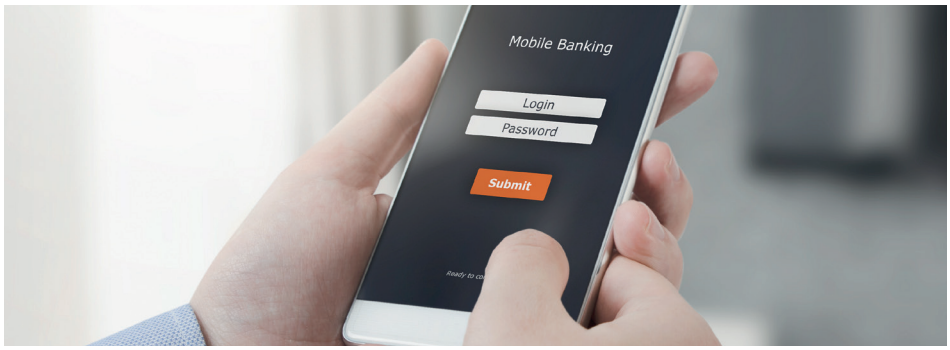
STRONG AUTHENTICATION FOR BANKING, TRADING AND MOBILE PAYMENTS

From mobile transactions to expanding regulatory demands in the European Union and beyond, the very nature of banking is changing at a rapid pace.

As new technology allows consumers and employees to interact with financial accounts in increasingly intricate ways, it is essential that financial institutions know who is involved in every transaction. Multi-factor authentication using biometrics provides the proof of identity that banks and other financial services organizations require. This not only enables them to keep up with the evolution of technology, but also stay ahead of hackers, fraudsters, and other criminals looking to exploit the confusion that comes with these rapid changes by securing and creating identity transparency.

Banking is Risky Business

Over the last decade, identity and financial fraud has risen dramatically, reaching an all time high in 2016 with 15.4 million Americans impacted by identity fraud. This rise in fraud is driven by increased accessibility to personal details and the volume of transactions in cyberspace, as more financial institutions migrate to digital services. In response, financial institutions are increasing their investments in cybersecurity, but many are playing catchup, rather than proactively working to stay ahead of hackers.



One of the primary drivers of this increase in fraud is ecommerce and Card-Not-Present (CNP) transactions, which grew by 40 percent in 2016 alone. Today, more consumers are shopping online and on their mobile devices than in brick-and-mortar stores, and many expect ecommerce to continue its rapid growth spurt, with a 23 percent year-over-year growth rate as of 2017. This accelerated pattern is leading to more CNP transactions, and a higher risk of card data being stolen or intercepted in transit.

What's Your Fraud Risk?

While many say that it's on consumers to ask themselves what their fraud risk is, banks need to as well. Because at the end of the day, it's the financial institution's responsibility when a customer is targeted with identity fraud.

Any financial services firm needs to assess their cybersecurity strategy and, more importantly, how their customers interact with their offerings, and determine where the weak links are.

For many, the biggest threat factor is likely customer authentication, and how their customers validate their identities. Passwords, PINs and tokens do nothing to show who a user is, just that they know the right secret phrase to gain access.

Optimizing Privacy for Security's Sake

Often, the discussion surrounding cybersecurity turns into one of "acceptable risk." No matter how strong we build security systems, it's only a matter of time and persistence for a hacker to infiltrate the system. That's why much of cybersecurity planning is determining acceptable losses – what can and can't be compromised. What's left out of the conversation is identity and privacy.

81 percent of data breaches involve weak and/or compromised credentials.

The fact is that by focusing on improving end user privacy –the security of user data and access control to it– financial institutions will be optimizing overall security at the same time. End user data and data-specific security is often the primary point of entry for any hacker - 81 percent of data breaches involve weak and/or compromised credentials. By improving end user privacy, security will follow.

Proving Identity for Financial Transactions

One of the best ways to enhance privacy is to change how end users authenticate and verify their identities.

Traditional methods don't provide you with any identifying information about who's on the other end of a transaction.

The challenge is that, at the end of the day, anyone could be using those types of credentials to access and account and approve a transaction. The only way to truly prove identity is to require stronger authentication methods – biometric authentication.

This strong authentication eliminates the age old problem of "on the Internet, nobody knows you're a dog," by providing a unique characteristic, indistinguishable from the end users themselves.

Truly Know Your Customer

One of the key requirements for financial services firms is Know Your Customer (KYC). As a primary deterrent for money laundering efforts, effective KYC solutions provide banks with incontrovertible proof of who is performing a transaction. Current laws and regulations surround KYC rely on knowledge-based authentication. Who are you? What documents do you have to prove who you are? Etc. But once an identity is established, the relationship relies on trust. You don't gain any actual proof of identity.

Biometric-based authentication provides that proof, allowing banks to truly know their customers.

As a truly unique identifier, biometrics have a clear advantage over passwords PINs, and security tokens by being an inseparable part of the end user that's impossible to forget and always proves who they are, not just what they know or have.

Achieve PSD2 Compliance

Going beyond KYC, however, is the EU's revised Payment Services Directive (PSD2). PSD2 alters the relationship that banks have with their customer data, requiring them to open it up to third-party services, such as ecommerce retailers and budgeting service providers, and the customers themselves. This access to information will be an important step in providing consumers with ownership of their own data, but increased accessibility also presents advanced security risk.

Strong authentication can provide the enhanced access management financials services providers need to secure customer data and protect themselves from data breaches, while meeting PSD2 requirements more easily.

Alleviate the Burden of Legal Non-Repudiation

The primary advantage that biometric authentication bring to the financial services industry, however, is achieving legal non-repudiation. Legal non-repudiation provides proof of integrity and origin of any financial transaction. In the past this was very difficult to achieve in the best of circumstances, and impossible in the worst.

The validation of a transaction by a third party is only as good as the third party itself, and reliance on digital signatures has obvious flaws, particular in the burden of proof of identity.

What biometric authentication offers is a prove identity beyond a shadow of a doubt and digitally sign a transaction with that proof, rather than a key or similarly non-identifying solution.

The Breadth of Biometric Authentication

Biometric authentication offers many benefits to financial services organizations beyond simply proving the identity of an end user. They create a simplified and personalized client experience, as you always know who is accessing your content and from where.

From simplifying user access to enhancing internal security, there are many significant ways biometric authentication can be deployed and utilized for identity and access management to boost overall security while making complex financial transactions easier to perform.

The continued growth of ecommerce, mobile financial transactions, and peer-to-peer payments has led to an increase in the demand for convenient security functions, primarily on mobile devices.

Beyond Touch ID / Apple Pay

This need for convenient security was what drove the rapid rise of Touch ID and its Android equivalents. The ability to unlock your device with a fingerprint, rather than a four-digit PIN or even longer passcode, has a lot of appeal. The continued innovation to bring this technology to mobile payment solutions like Apple Pay was the obvious next step. As more retailers began accepting Apple and Samsung Pay, consumers wanted the convenience that their fingerprint brought to unlocking their device.

But at the end of the day, is approving a financial transaction with a mobile fingerprint better than a PIN code you can forget or have stolen?

Mobile fingerprint sensors embedded in devices only capture a partial print – a strip across the finger – rather than an entire, complete print. This means you're only using a portion of your fingerprint, and therefore only a portion of the security it can provide, to approve that purchase. More complete biometrics, such as new iris recognition capabilities and touchless fingerprint capture, offer a greater degree of security for mobile payment apps.

Biometrics for Strong Authentication

Beyond mobile payments, mobile biometric authentication offers a significant security improvement for internal operations at financial institutions as well.

Particularly in high value trading, proving a trader's identity is critical for legal non-repudiation, while being able to do so quickly boosts productivity and security.

Currently, passwords and tokens provide two-factor authentication for additional layers of security, but financial institutions need strong authentication to protect network and data access and other sensitive systems.

Transaction Signing

For both PSD2 compliance and legal non-repudiation needs, biometric authentication provides transaction signing.

The ability to add a digital signature to any transaction type that includes more proof of identity than a password, PIN, or e-signature is able to provide ensures that the record can be verified and is ready for security and regulatory audits in the future.

Furthermore, biometrics add the ability to simplify transaction signing in the digital age, when other solutions are cumbersome or require remembering a difficult code or phrase, making it more convenient for end users at the same time.

Mobile Authentication with VeridiumID

In order to address the need for strong authentication that includes more complex biometric data than Touch ID and its Android equivalents are capable of, Veridium developed its own suite of identity and access management technologies, including 4 Fingers TouchlessID.

By focusing on the mobile devices –something everyone has on them at nearly every hour of the day– and eliminating limiting factors such as hardware fingerprint sensors, we worked to produce a biometric authentication platform that has broad compatibility and simplified user adoption to minimize the challenge of acquiring strong authentication on a mobile device.

The result is a contactless fingerprint solution that captures four complete fingerprints simultaneously, creating a standard for mobile fingerprint capture that doesn't limit end users to a particular device or operating system.

A BIOMETRIC FUTURE

Veridium's solutions address a variety of use cases for strong biometric authentication in financial services that improve security and enhance usability across the board.

Cardless ATM

From checking your balance to withdrawing money from an ATM, mobile biometric authentication opens up new doors for security and convenience by eliminating debit cards and PINs from the equation. Customers will be able to access an ATM using their mobile device and process and approve a transaction using their biometrics, rather than a PIN they could forget or have stolen. This also eliminates the risk of card skimmers used to steal account credentials at the ATM.

Mobile Banking

Biometric authentication can provide secure bank account access for customers while eliminating security risks associated with passwords. This optimizes the convenience for your customers to access their finances but keeps you in control of authentication, unlike Touch ID and its counterparts. VeridiumID also allows for multiple biometric modalities to be used, supporting various levels of security. For accessing account balances, customers could still use Touch ID, but for making higher value account transfers, you could request stronger authentication with 4 Fingers or iris. The solution allows you to track risk, value, and location, so that you can build a complex authentication process that's seamless and enhanced for the end user.

POS Terminal Authentication

POS terminals are becoming more advanced, with cameras built in or at the kiosk, as well as supporting mobile payments and similar technologies. VeridiumID offers the option to expand these capabilities with biometric authentication, removing the need for hardwaresupplied terminals and allowing small businesses to enable their own mobile and tablet POS environments. Using a mobile app for payments, rather than a card and terminal, you can secure the payment process at the same time as making it faster and more convenient for customers.

High-Value Trading

Trading is a high-risk arena already, but the lack of proof (legal non-repudiation) on a trade makes it even riskier. If a large trade moves in the wrong direction, a trader could say, "it wasn't me, I didn't make place that trade. Someone must have done it from my terminal." Biometric authentication eliminates this risk, "signing" the trader and the action to provide a record of the transaction. This will reduce fraudulent trading by achieving legal nonrepudiation on every transaction and create electronic records of every account session including the person, their IP address, and the time of the transaction.

Digital Identity

Biometric authentication can also be used within identity service providers as the "identity custodian." When an identity offering is requested, VeridiumID can step in to provide identity services using biometrics and strong authentication to ensure the end user is who they claim to be. This will reduce fraud and validate users for access requests in any medium. This would include a capability for AML/KYC processing, and also resolve GDPR and PSD2 data management and policy regulations.

CONCLUSION

In order to prepare for the uncertainty in banking arriving over the next few years organizations need to consider what their access management solution is as a whole.

Are you using biometrics to prove identity and address the threat of fraud?

Does it help you achieve KYC and regulatory compliance?

Does it support legal non-repudiation?

By going beyond existing security methods and embracing biometric authentication, banks can do all of these things, and more.

The VeridiumID platform provides all of the necessary resources for an integrated biometric solution as part of identity and access management.

You can created tiers of login security based on access and security needs, requesting different biometrics, or combinations of biometrics and other factors for multi-factor authentication.

Combinations of what you know, have, and are (password, smartphone, and biometric) can provide the stronger proof of identity needed for modern cybersecurity and still keep access convenient for customers and employees.

VERIDIUM
TRUSTED DIGITAL IDENTITY

London
119 Marylebone Rd
North West House
London NW1 5PU
United Kingdom
+44 1753 208780

Oxford
The Magdalen Centre
Robert Robinson Avenue
Oxford Science Park
Oxford OX4 4GA
United Kingdom

New York
1325 Avenue of the Americas
28th Floor New York 10019
United States of America
+1-857-228-7805

Romania
Bucharest
Buzesti Street 71

Press Contact
info@veridiumid.com
+1-857-228-7805

www.VeridiumID.com