Beyond Passwords

How Banks and Financial Firms Can Address Customer Security with Convenience

ARCULUS

KEY FINDINGS:

Cybercrime & Fraud

Cybercrime and fraud continue to pose significant challenges, with the FBI estimating that losses to U.S. citizens topped $10 billion in 2022.

Phishing Schemes, Scams & Attacks

Far too many banking customers rely on weak or compromised passwords for their security, allowing fraudsters to gain access to money and data through phishing schemes, social-engineering scams and brute-force attacks.

Compromised Authentication Methods

While two-factor and multifactor authentication provide better security, these methods are also prone to compromise and add friction to customers' banking experience.

Modern Security Reduces Fraud & Losses

Modern, more convenient security solutions, such as those offered by Arculus and based on proven FIDO2 standards, help reduce fraud and losses from cybercrime.

CURRENT STATE:

The FBI estimates cybercrime losses now top $10 billion. With weak passwords that play into fraudsters' hands, banks and their customers need secure yet easy-to-use solutions to protect their money, identity and data.

Even before the COVID-19 pandemic, banking customers increasingly wanted a more digital and frictionless experience when it came to accessing their money and other financial services. A 2023 survey published by Forbes found that 78% of adults in the U.S. now prefer to bank through a mobile app or website.

The same Forbes research found only 29% of Americans need or want to bank in person, showing consumers are now comfortable with a digital-first and mobile-friendly approach to their personal finance.

As banking and personal finance services have become digital–and as consumers increasingly rely on payment cards and online services for their transactions–fraud and cybercrime are increasing. The FBI's 2022 Internet Crime Report notes that their agents received more than 800,000 complaints about cybercrime in 2022 and that total losses to American citizens likely exceeded $10 billion.

$10 Billion

Cybercrime losses topped $10 billion in 2022

Cybercrime and fraud continue to increase because consumers who are eagerly embracing digital banking services also rely on traditional password security to access their accounts and data and protect their identity.

"We've gotten to the point where passwords are just broken. It's just a broken technology at this point."
–Tom D'Eletto, Head of Product for Arculus

The use of weak and compromised passwords as well as lack of additional security plays into the hands of cybercriminals who compromise and steal these credentials through several means such as phishing email attacks, social-engineering ploys and SIM-swapping.

The weakness of passwords for robust security is well documented. Microsoft's Digital Defense Report 2022 finds that password attacks reached 921 incidents every second–a 74% year-over-year increase.

"We all agree that passwords alone are highly problematic," says Tom D'Eletto, Head of Product for Arculus, a custom digital security solution by CompoSecure. "People reuse passwords. They use weak passwords and we almost always force people into situations where they end up creating crazy passwords that they can never remember."

As cybercrime losses total into the billions, reliance on passwords and other security factors that do not require strong authentication fails to protect customers in the banking and financial sectors. Even newer methods such as two-factor or multifactor authentication are not enough to prevent cybercriminals from taking advantage of weak security and compromised credentials.

There is also a convenience factor for banking customers, who want to access digital services with the same frictionless experience as using a payment card to withdraw money from an ATM. What's needed, instead, are modern solutions based on the best elements offered by the FIDO Alliance through the organization's FIDO2 open standards for online authentication.

This approach reduces the need for passwords but provides the same seamless convenience for bank customers who don't want to carry additional hardware or switch from various platforms to authenticate their identity to access the financial services they need.

Identity Theft and Data Breaches: A Continuing Cybercrime Problem

As the FBI's latest Internet Crime Report makes clear: Cybercrime is not going away.

While an increasing amount of the FBI and law enforcement efforts over the past two years have focused on headline-grabbing incidents such as ransomware and business email compromise (BEC) attacks, the latest bureau statistics show that complaints about personal data breaches topped 58,000 reported incidents in 2022, while identity theft claims accounted for nearly 28,000 complaints sent to agents.

In terms of damage, personal data breach scams and fraud accounted for over $742 million in losses in 2022, while identity theft accounted for $189 million, according to the FBI.

The three-year-old COVID-19 pandemic and the increasing reliance on digital services of all kinds, including banking and other financial services, are only accelerating these trends. In fact, the 2023 Verizon Data Breach Investigations Report looked at more than 1,800 incidents in the financial and insurance industries and confirmed that 480 of these involved some type of confirmed data disclosure.

$742 Million

$742 million lost to data breach scams and fraud in 2022, while identity theft accounted for $189 million

Verizon researchers found that in 97% of these incidents, financial gain was the main motive and the type of data compromised included personal data (74%), passwords or credentials (38%) and banking information (21%).

"The top three patterns remain the same, but their order of ascendancy has rearranged. Personal data, very useful for fraud, continues to be the most desired data type stolen," according to the Verizon DBIR.

Identity theft and breaches involving personal data, along with compromised credentials and weak security protections, have also resulted in more account takeover schemes by cybercriminals–a significant concern for banks and other financial institutions.

Account takeover schemes typically involve threat actors or cybercriminal groups who access legitimate bank accounts, hijack those accounts and change information and passwords. Once the legitimate account owner is locked out, fraudsters can gain access to money or data. A report in SC Magazine, which cites data published by Javelin Research, found that account takeover attacks increased by 90% between 2020 and 2021, resulting in over $11 billion in losses.

"It's a growing problem that has expanded in new ways since the onset of the COVID-19 pandemic, which prompted wide changes in digital behaviors," the Javelin Research report noted.

In turn, the large payoffs from identity theft and account takeovers help fuel an increasing array of cybercriminal activity that traffic in compromised credentials and reused passwords that can access personal accounts and data, including:

- Brute-force attacks
- Malware
- Phishing attacks
- SIM-swapping
- Social-engineering schemes

When looking at these increases in cybercrime and fraud, the main culprit remains the reliance many banking consumers have on weak password security–as well as the use and reuse of compromised passwords and credentials–giving cybercriminals a distinct advantage.

Why Relying on Passwords Compromises Security

For years, cybersecurity professionals have warned that weak and reused passwords compromise security and leave consumers and businesses open to any number of threats, whether it's phishing email attacks, BEC schemes, ransomware or breaches.

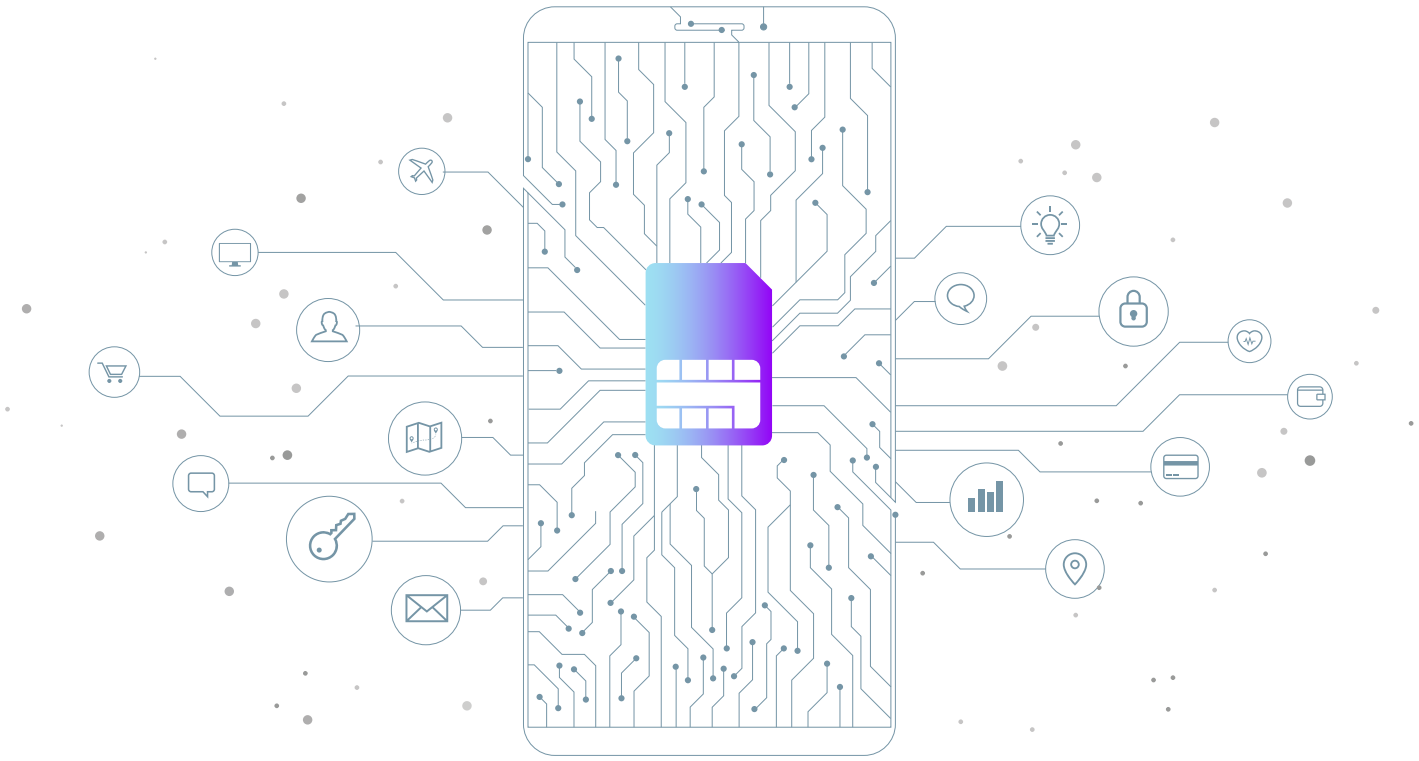
With nearly every website or application requiring a password, consumers typically reuse the same password over and over again, making brute-force attacks that guess these credentials a systemic problem.

Many of these brute-force attempts are fueled by phishing sites that vacuum up passwords and credentials consumers willingly give away. The Anti-Phishing Working Group, a tech-industry nonprofit, found that phishing sites hit an all-time high–1 million sites–in the second quarter of 2022.

"This is why security experts are always telling consumers not to reuse a password on sites: Because if one site does a bad job of securing that password and it gets out into the world, you haven't just lost the password for that site. You lost the password for all the places where you use that password,"D'Eletto says.

Users, and the websites and applications they rely on, need better tools to ensure that credentials are secure. The Microsoft Digital Defense Report concluded that password attacks are closing in on 1,000 attempts every second. In addition, 90% of these involve accounts that lack "strong authentication," meaning two-factor or multifactor authentication.

Even with the additional protections afforded by two-factor and multifactor authentication, cybercriminals have found ways around these security features. For instance, the FBI has warned publicly since at least 2019 that cybercriminals increasingly use social engineering techniques to bypass multi-factor authentication.



This includes a noticeable increase in SIM-swapping incidents, where a threat actor takes a victim's phone number–typically by using social-engineering techniques on carriers' customer support personnel–and port the number to another SIM card that is under the control of the attackers, who can receive one-time passwords.

SIM-swapping is now big business. The FBI finds that the bureau received more than 1,600 complaints in 2021, with losses totaling $68 million. In the three years prior, agents recorded only 320 SIM-swapping complaints, according to The Wall Street Journal. The results show that sometimes even the best intentions to secure data and identity come up short.

"Unfortunately, a lot of these two-factor authentication measures we use are also weak. Security protections such as emails are weak. SMS messages are weak because if someone hacked your account, guess who's getting that second factor? The hacker who hacked you in the first place. So security folks know why email and SMS two-factor are also terrible. It's better than passwords alone, but it's not strong enough for what it's protecting, and it's also a poor experience," D'Eletto says.

Increasing security, as well as improving the customer experience, is why the FIDO Alliance and its partners, such as Arculus, are looking to drive industries such as banking and finance into adopting FIDO2 standards that offer better protection for consumers and lessen the reliance on passwords and third-party applications to provide security.

Why Now Is the Time for Fresh Approaches to Security

In response to increases in fraud and cybercrime, there has been an uptick in adopting security standards backed by the FIDO Alliance and its members and based on FIDO2 authentication standards.

One of the most visible is passkeys, which are based on WebAuthentication. While one of a pair of keys is publicly stored in a server, the other private key is not. Instead, a customer can use his or her mobile device–Android or iPhone–to complete the authentication process and log into a web application or another device such as a laptop. The Wall Street Journal notes that with Google and others backing this approach, the use of passkeys is growing, albeit slowly.

The drawback, as D'Eletto describes it, is that passkey methods rely significantly on a USB key or another type of hardware device the customer must carry to authenticate their identity. While more secure than traditional passwords and multifactor authentication, relying on a dongle or another device adds a layer of expense for the user and creates friction throughout the process.

"I think passkeys are a good thing. We've been talking about moving away from passwords for a couple of years now, and I think we're finally at the point where we're getting real traction on that, and I think passkeys are a big reason why we're finally getting real traction on that," D'Eletto says. "But I also look at it and think that part of the problem with hardware keys traditionally has been that type of artificial scarcity. People don't want to go out and buy them, and they're weird devices, and that's really why they haven't found mainstream success."

The next wave in secure authentication is one based on FIDO2 standards but that offers convenience for consumers, as well as for banks and other financial institutions that need to provide frictionless experiences. This approach includes a premium metal payment card powered by Arculus authentication technology, based on those advanced FIDO2 standards.

The combination of Arculus security technology with the premium metal payment card that financial organizations can brand and distribute to their customers provides two significant advantages for banks, their security teams and their customers:

- Cardholders can tap their secure authentication card to their smartphone to log in and make payments. This increases customer interaction with their bank or financial institution and the metal form factor gives the added benefit of a premium brand experience.
- On the security side, customers do not need to buy additional devices to benefit from the increased security of hardware keys. The premium metal payment card can be used as a hardware security device simply and securely.

"By bundling it with a card, we remove that scarcity," D'Eletto says. "Your bank has already given you a card. They can make that card also be your hardware key. So instead of being a generic device where I have this one USB dongle that I use to log into everything, I can use my Chase card to log into Chase. I can use my Fidelity card to log into Fidelity. I can use my Coinbase card to log into Coinbase. I no longer have this artificial scarcity where if I have one USB FIDO key, I better not lose it."

Perhaps most importantly, the combo premium metal card and Arculus technology gives banks a clear path to allowing customers to go truly passwordless: By using the metal payment card with Arculus Authenticate, customers will seamlessly log in with their biometrics–if needed or required–PIN and tap their card in combination with their smartphone.

"It's much more convenient because you don't have to leave the app," D'Eletto said. "It's an experience that you're used to from going to an ATM. I put in my PIN. I tap my card. I get my stuff. I don't have to actually leave the banking app to go to some other app to do anything. It's more secure and it's more convenient."

KEY TAKE-AWAYS:

Cybercrime & Fraud Prevail

Cybercrime continues to challenge the banking industry and law enforcement. With losses topping $10 billion, consumers need better protection when it comes to securing their money and data.

Passwords are Outdated & Two-Factor Limited

Using passwords is an outdated security measure that is easily bypassed by cybercriminals and fraudsters through phishing, social engineering and other schemes. Even two-factor and multifactor have limits.

Go Passwordless. Go Securely. Go Arculus.

Embracing FIDO2 standards and combining these with the convenience and frictionless experience of premium metal payment cards that utilize the Arculus Authenticate, offers customers a way to securely go passwordless while giving banks added layers of security for the clients they serve.

LEARN MORE:

Reach out to us at b2b@arculus.co to schedule a demo and to learn more about how Arculus Authenticate can work for your business.

Arculus is a trusted leader in passwordless security, developed by CompoSecure–the world's leading producer of premium metal payment cards. Our fully customized security solutions are user-friendly and simple.