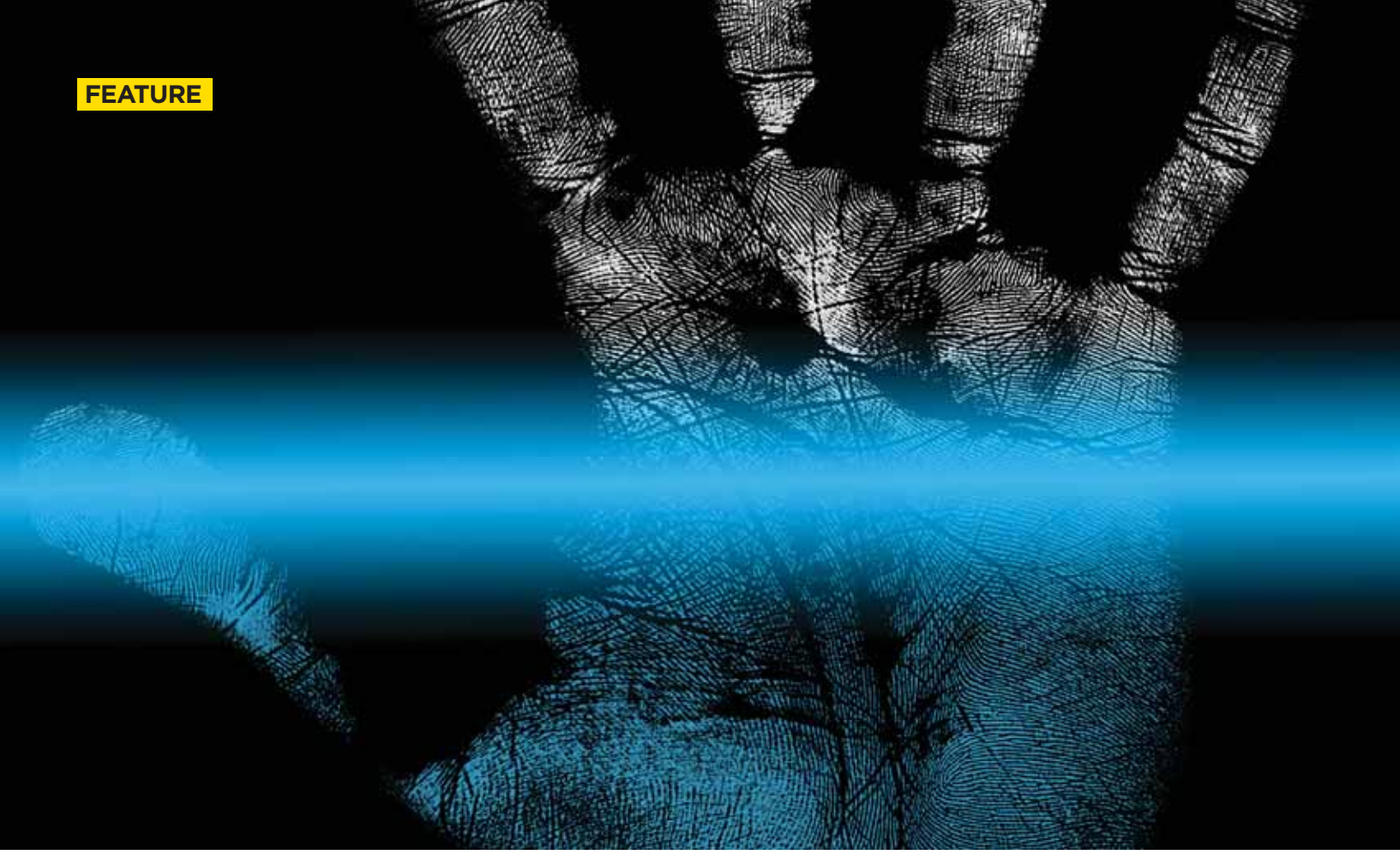
FEATURE



SMARTPHONES SPUR BIOMETRIC ATM AUTHENTICATION

With the rise of 'mobile-first' consumers, *Robin Arnfield* investigates how smartphones may be the future for biometric authentication at ATMs

Integrated biometric readers are widespread at ATMs in Brazil, India and Japan, while European and North American ATM operators haven't yet deployed biometrics, with the exception of Poland, Russia and Turkey.

"Most Japanese ATMs have fingerprint/ finger-vein or palm-vein scanners", says biometric security expert Douglas Russell, director of DFR Risk Management.

Russell explains that many biometric ID initiatives in developing markets involve extending financial inclusion. "For example, Brazil's Bolsa Familia (family allowance) program originally required cards and PINs for benefits withdrawals at ATMs," he says, "but as many recipients were unfamiliar with ATMs, they frequently forgot their PIN. So fingerprint scanners were deployed to replace PINs."

In developed markets, where ATM card-skimming is a major issue, security is the driver for banks to adopt biometrics. "Biometrics help prevent card-skimming with features like likeness detection to guard against biometric 'copies' such as fingerprints lifted from glass surfaces", Bob Konecny, Diebold Nixdorf's advanced technology incubation manager, says.

For consumers, the convenience of biometrics is a driver. "Biometric credentials are part of a consumer and always available, as they can't be lost or forgotten," argues Konecny. "So they remove the need for PINs and passwords."

Obstacles and Barriers

Obstacles to biometric ATM adoption include different attitudes to personal privacy in various markets, plus different generational attitudes to biometric technology.

"Japanese people prefer palm-vein to other biometric methods, as there's no physical contact, and they're concerned about hygiene," says Ben Knieff, a consultant specializing in financial fraud at New York-based Outside Look. "In Europe, personal privacy is important. Biometric data, despite being encrypted and hashed, feels too personal to Europeans, so they wouldn't want biometric ATMs."

Knieff says the barrier in the US is people's concern about the government obtaining their fingerprints, "but in Asia and South America, people think governments already have all the data they need about them, so they have nothing to lose from biometric ID."

"In some countries, older people still link the idea of providing their fingerprints to a bank with criminality", adds DFR's Russell.

However, young people accustomed to doing everything on their smartphones don't share this concern, particularly as smartphones offer fingerprint sensors like TouchID and facial recognition apps.

"There's a generation of young people who aren't as concerned about privacy as older people, as they already chose to give up their privacy online and do selfies," Knieff says. "Their attitude is 'my biometrics are already out there, and I put them there.' So barriers against biometric ID are beginning to disappear in Europe and North America."

Mobile Authentication

Developments in mobile banking and payments may help drive consumer acceptance of biometric ATMs.

For example, Apple Pay requires fingerprint authentication, while US banks such as Wells Fargo and Chase offer biometric authentication for mobile banking apps. Banks are also rolling out cardless ATM access services for smartphones using Near-field Communications (NFC) and Quick Response (QR) codes.

Surveys indicate that consumers are enthusiastic about replacing banking passwords with biometrics. A March 2017 survey of 1002 US adults for EyeVerify's Retail Banking *Biometrics Confidence Report* found that 42% of respondents would not use banking or payment apps that don't offer biometric authentication.

"Customers can log into our mobile banking app via TouchID and Android Fingerprint ID," a Wells Fargo spokesperson says. "Once you're authenticated via your fingerprint, you can perform a cardless ATM withdrawal using your phone at our ATMs."

The Cost of Biometrics

Biometric systems, particularly scanners, have fallen in price as the volume of biometric deployments has increased. The challenge lies in deploying and managing the necessary biometric ATM infrastructure including customer registration and databases.

"The physical hardware cost for biometric readers isn't significant," says Owen Wild, NCR's global marketing director for fraud and security. "The cost lies in the integration and configuration of the technology at ATMs and associated biometric databases, which is more challenging than using smartphones for biometric authentication."

Biometrics will gather momentum in all areas of consumers' interaction with banks, and we'll see more ATMs with integrated biometric scanners, adds Russell, "but because integration is easier, smartphone-based cardless transactions using fingerprint scanners will likely see the highest deployment for biometric authentication at ATMs."

If banks deploy biometric scanners in their ATMs, they can only use the technology with their own customers, unless they exchange customers' biometric data with other banks. Also, due to lack of global biometric standards and databases, biometric scanners at ATMs can only be used by domestic users.

"For biometric ATMs to be truly international, more work needs to be done on creating global standards", says Russell.

"ATM biometrics adoption has been limited to countries where there are only a few large banks cooperating to implement biometrics," adds Konecny. "For example, in Brazil, where the market is dominated by five or six major banks, over 85,000 ATMs are outfitted with biometrics."

Another example is India, where biometric ATM adoption has been aided by the country's nationwide Aadhar biometric ID scheme. The 12-digit Aadhaar card number is linked to India's demographic and biometric information and a government-issued photograph.

Registration in the Authentication Chain

"Enrollment – generating the user's biometric template (the digitized form of users' biometrics) – could be done at ATMs without supervision," says Russell. "My preference, however, is for supervised enrolment. Supervision means staff can educate customers about their system, increasing accuracy of gathering biometric characteristics and providing opportunities to verify the identity of customers being registered."

However, registration represents the weak point in the biometrics authentication chain.

"If someone steals your information, signs up for a bank account and enrolls their fingerprints under your name, how do we check whether this biometric identity is actually yours?" Knieff asks. "The number of times the biometric registration process will be compromised is relatively low, but it can happen. So it's vital to correctly tie biometric identities to real identities. One solution is to look at behavioral

Fiserv Deploys Palm-vein Authentication

Fiserv has introduced Verifast: Palm Authentication based on Fujitsu's PalmSecure palm-vein technology to combat branch and ATM fraud.

"Using palm-vein authentication at bank teller stations is faster than using debit cards for identification," says Chris Van Der Stad, Fiserv's SVP, open solutions. "The in-branch registration process takes 15-20 seconds. Also, there's no way biometric skimmers can copy the pattern of veins on a user's palm, which has millions of unique reference points."

Fiserv is working with several ATM vendors to add Verifast to their ITMs (Interactive Teller Machines). An ITM is an ATM with the ability to videoconference with remote tellers.

"Our clients' experience is that Verifast is attractive to older customers, for example if they walk with a cane and can't easily get their card out," says Jaime Dominguez, Fiserv's director of strategy, retail banking and channels, bank solutions. "If our clients have licensed Verifast from us, the cost for them to add biometrics to their ATMs won't be dramatic", he adds.

attributes and check whether you can identify previous behaviors with this current enrolment."

False Positives/Negatives

"Most biometric systems have the ability to configure an acceptable level of false positives and false negatives", Russell explains.

"The risk of false positives with biometric ATMs is miniscule compared to that of false negatives, which is much more common," adds Knieff. "For example, a fingerprint sensor may not work if the user's finger is sweaty, so they'll be asked to keep trying. It's one thing if that happens on your iPhone, but it's different if it happens when four people are behind you at an ATM."

"Multi-factor authentication will be key," says Diebold Nixdorf's Konecny. "When combining face and voice biometrics, accuracy approaches 99.9%, according to some studies."

In terms of skimming, the risk of customers' biometric credentials being skimmed at ATMs could be justification for banks to opt for biometric authentication via smartphones instead of through ATMs.

"Performing biometric authentication on smartphones for ATM transactions alleviates privacy concerns over where the biometric template is stored", says Konecny.

In October 2016, Kaspersky Lab warned that at least 12 sellers were offering ATM skimmers capable of stealing victims' fingerprints. "Hackers have devised skimming technology that can capture fingerprints, iris recognition and palm-vein data," says David Vergara, Vasco Data Security's head of global product marketing.

"With biometrics theft, more is at stake than stealing cash, as criminals can perform ID theft," Sergey Golovanov, Kaspersky's principal security researcher, says. "Compromised cards or PINs can be changed by customers, but biometric data isn't modifiable and can't be revoked if compromised."

There are two biometric data theft scenarios:

1. Banks' biometric readers connected via USB/serial ports might be hacked, and data transmitted could be intercepted and stolen
2. Attackers can attach biometric data skimmers to ATMs to steal authentication data

Once hackers obtain biometric data, they can use it to authorize other bank services such as web banking, perform fraudulent online transactions or sell biometric data on the black market, Golovanov warns.

ATMs of the Future

"Putting staff into branches is expensive, so the future will see ATMs positively identifying customers with biometrics, so clients can engage with remote staff over video links and apply for bank products", claims Knieff.

The ATM of the future will be a banking center offering multiple day-to-day transactions, so branches can focus on customer service and sales, adds NCR's Wild. "ATMs may not have keyboards, just a secure safe, and customers will interface with them via mobile wallets and NFC or QR codes."

"In the future, there will be diversity of ATM biometrics," says Konecny. "Outdoor ATMs affected by adverse lighting and sound will focus on touch-based systems like fingerprint or finger-vein. Indoor terminals will focus on passive biometrics such as voice recognition, as the conditions can be much more controlled." END

Biometric Authentication

In June 2017, ATM vendor Diebold Nixdorf partnered with Samsung SDS America to deploy Samsung SDS Nexsign biometric authentication for cardless/PINless ATM withdrawals. The firms said customers tap their smartphone against the ATM's NFC reader, authenticating themselves via facial recognition on their phone. Banco Popular, Puerto Rico's largest bank, plans to pilot this authentication method in summer 2017.

Case study: Bradesco

Brazil's Banco Bradesco deployed palm-vein biometrics at its ATMs in 2007. "Currently, we have 16.7 million customer accounts which have activated palm-vein biometrics for ATM access", Fabrizio Pinna, Bradesco's executive superintendent for digital channels, says.

Bradesco uses Fujitsu's PalmSecure sensors, which it has rolled-out across its entire Brazilian ATM network.

"Customers can use just biometric authentication plus their PIN without their card or smartphone," a Bradesco spokesperson says. "Or they can use their card and biometric authentication without their PIN."

"Today, 100% of our banking services can be carried out simply by using biometrics at ATMs," says Pinna. "In 2016, we launched cardless ATM withdrawals via NFC, which allows customers to prestage ATM transactions in our mobile banking app and then use NFC combined with biometrics at our ATMs."