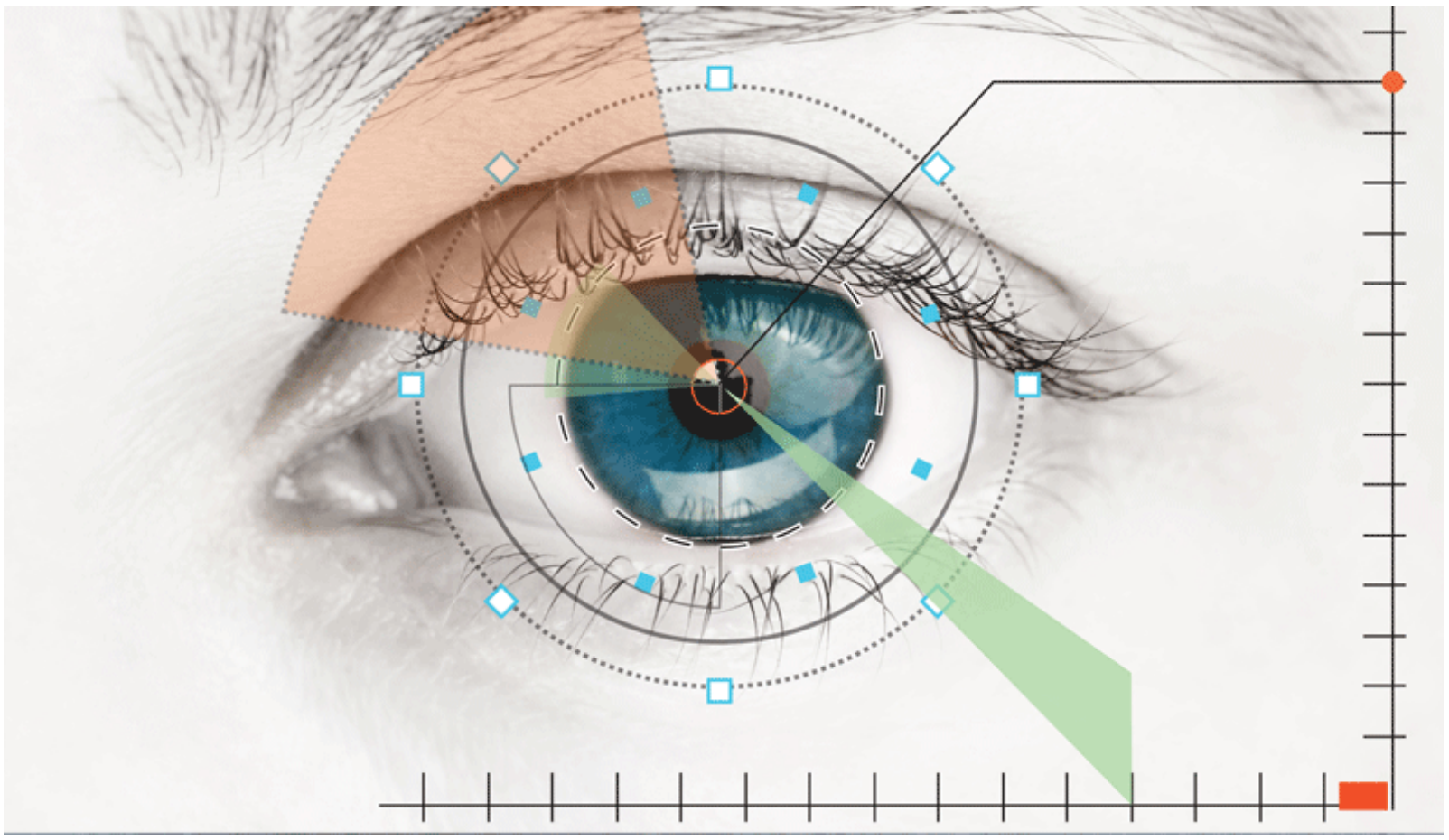
# Atlanta Fed Conference Explores Biometrics in Payments

December 3, 2015



Iris scanning, face and voice recognition, even vein detection. It all sounds thoroughly futuristic. But the future is now, at least in the payments arena.

The use of physical characteristics to identify people—biometrics—is older than flying machines. Seeking a way to identify repeat criminal offenders so as to mete out harsher punishments, a police inspector in England in the 1880s devised a system of measuring criminals' arms, heads, and other features. Then crime fighters began fingerprinting suspects a couple of decades later.

Today, a smart phone can have a fingerprint reader to prove you're you when you make a payment over the phone. Consumers can now choose from more than a dozen "mobile wallets," essentially payment mechanisms built into mobile phones. Numerous big technology and financial firms have rolled out payment apps that use biometrics. And many information security experts contend, as a panelist at a recent Atlanta Fed conference proclaimed, that it is time to retire passwords as an authentication tool.

Even so, biometrics today authenticate only a tiny fraction of payments in the United States, according to the Atlanta Fed's Retail Payments Risk Forum. Part of the reason is that biometrics are used almost exclusively in mobile payments—those made mainly with smart phones—and these transactions still account for a small percentage of U.S. payments.

## Ground becoming fertile for mobile payments, biometrics

"But it's going to grow," said Dave Lott, payments risk expert in the Atlanta Fed's Retail Payments Risk Forum. "The ground is becoming more fertile."

It's far from certain, but a boom in mobile payments and biometrics, long promised by industry boosters, could be dawning. That was among the themes that emerged from the Risk Forum's November forum, "Banking on Biometrics: Bye-Bye Passwords?" The one-day forum explored the present and potential of biometrics as a verification tool for payments and banking.

economymatters

ANNUAL REPORT

ECONOMIC RESEARCH

BANKING & FINANCE

REGIONAL ECONOMICS

COMM/ECON DEV

INSIDE THE FED

DEPARTMENTS

Financial Tips
Podcast
Quizzes
Staff & Credits

Subscribe to e-mail updates

Dave Lott, payments risk expert in the Atlanta Fed's Retail Payments Risk Forum

Photo by Odie Swanegan

## Something you have, something you know, something you are

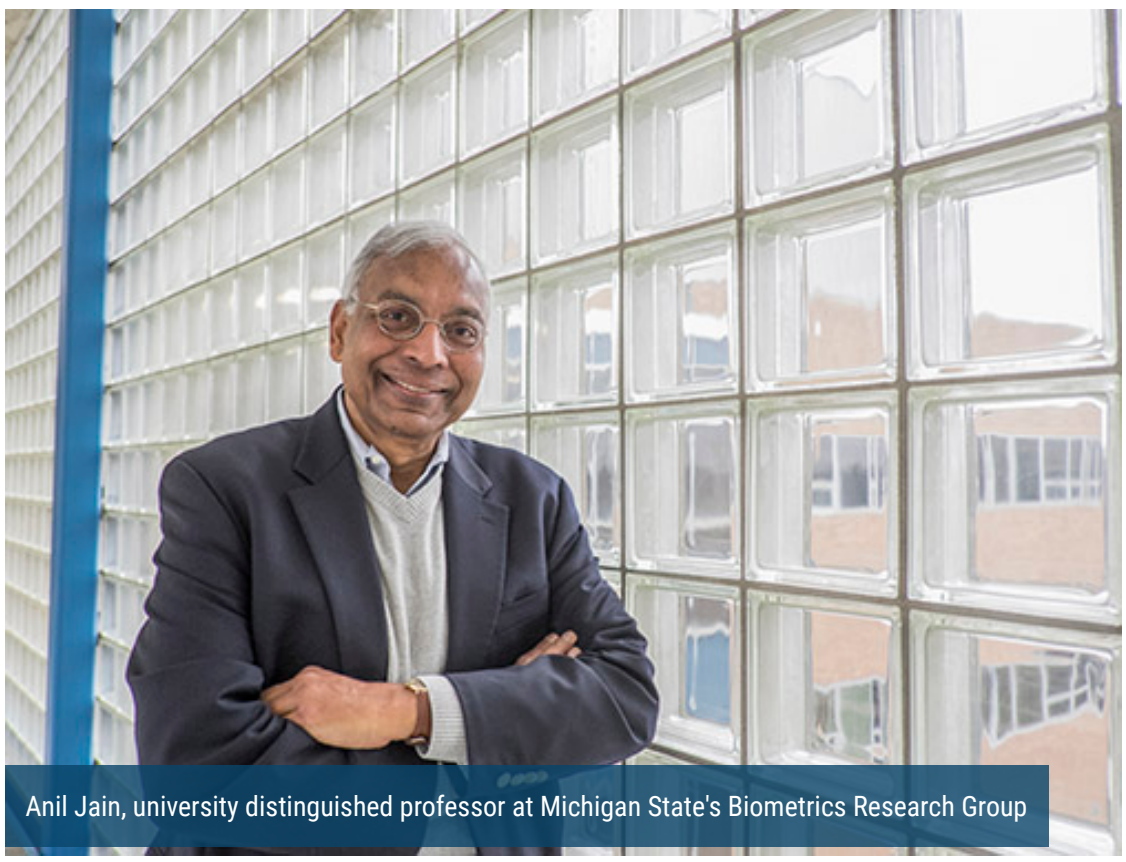
Verifying a person's identity generally encompasses some combination of three elements:

- Something you have (a payment card, for example)
- Something you know (a PIN or password)
- And something you are (your fingerprint, iris, and so on)

So far the first two have served the U.S. payments system reasonably well, Lott pointed out.

That may be changing. For several reasons, security experts consider passwords a weak form of authentication. In part, that's because it's up to consumers to devise strong passwords, and most simply don't make them strong enough, Lott said, even though people in surveys overwhelmingly express concern about the security of their information.

As passwords gradually fall out of favor, several currents appear to be favoring a rise in the use of biometrics. For one, the technology has improved dramatically. Early facial recognition systems in the mid-1990s, for example, erroneously rejected a person about 79 percent of the time, according to tests by Anil Jain, keynote speaker at the Atlanta Fed conference and university distinguished professor at Michigan State's Biometrics Research Group. By 2010, the false rejection rate was down to 1 percent.



Anil Jain, university distinguished professor at Michigan State's Biometrics Research Group

Photo courtesy of Michigan State University

## Ensuring faces, fingers are alive

Some of the technological advances are fascinating. Many sensors now include "liveness" detection. For instance, many facial recognition sensors require that you blink to be sure your face picture is real and not a three-dimensional mask, and advanced fingerprint readers detect blood flow.

Meanwhile, consumers have become more receptive to biometrics, Jain said. That growing level of acceptance seems to be evident in the marketplace. USAA, the first financial services firm to offer fingerprint, voice, and facial recognition for mobile banking apps, has garnered more than a million users for its biometric system since its January introduction, according to the company. That rate of adoption puts it ahead of schedule, said conference panelist Conor White, whose company, Daon, supplies USAA's biometric technology. MasterCard in October introduced a technology that allows shoppers to authorize a purchase with a snapshot of their face.

And smart phone payment systems appear to be catching on. Jain said Apple Pay is supported by more than 300 banks, while

Android Pay is accepted at more than a million stores.

"Biometrics are changing the way we conduct everyday transactions," Jain said, "and now the focus is on payments."

Nothing, including biometrics, promises 100 percent security, according to Jain and other conference speakers. In fact, most suggested the best security comes from using multiple forms of biometrics and other authentication elements. One of the keys to solid authentication, several conference speakers noted, is to figure ways to block imposters even if they have compromised biometrics, which sometimes can be done with photos or even 3-D masks on less-sophisticated systems.

A few snags have traditionally held back wider adoption of biometrics. For example, a person's fingerprint is never read as identical, Lott explains. There's almost always a tiny difference, be it because of cuts on the finger, the angle of the finger, how hard the person is pushing down, and so on. A password, on the other hand, is either right or wrong, cut and dried, every time. But fingerprint readers, like all biometric devices, are getting better.

The real key to biometrics becoming ubiquitous is straightforward, said conference panelist Vijay Balasubramaniyan, cofounder of an Atlanta-based company called Pindrop Security that develops voice authentication systems for call centers: they must offer real security and be easy to use.

---

**Charles Davidson**
Staff writer for *Economy Matters*