



Are Biometrics Next Up in Fight for Financial Security?

U.S. financial institutions are slow to adopt biometrics, but for good reason.

By Karen Krebsbach
December 22, 2003

Overseas, financial institutions have been very proactive in using biometric products and services for everything from employee verification to consumer authentication. In Europe, where ID fraud is taken as seriously as it is in the U.S., most countries include a biometric fingerprint on their driver's licenses. Not so in the U.S.

Analysts say U.S. banks are taking longer than their overseas brothers to adopt biometric options, given their concerns about accuracy, affordability, security, and convenience. Financial institutions in this country are slow to embrace biometrics because they're wedded to their IT legacy systems and are reluctant to start over with what many still consider untested technology.

Biometrics has been especially popular in Latin America and Eastern Europe because existing safeguards are so far behind U.S. technology that they have a lot of catching up to do, says Ed Kountz, TowerGroup senior analyst. They can just leapfrog over where they would have been, so it's not as much of an investment, he says.

"What's happening in biometrics in the U.S. is similar to what happened with mobile technology," Kountz explains. "The cell phone revolution grew much faster in Europe than in the U.S. because we have an established infrastructure [of land lines] that basically works. So what's the value of changing the system? Is there enough fraud or risk of fraud to worry about?" Many argue there is now. Financial institutions might be waiting for broader consumer acceptance before adopting biometrics more widely.

Various European countries have already instituted national ID cards with fingerprints attached, including Belgium, Portugal, and Germany. Last month, the British government announced plans to introduce compulsory biometric ID cards using fingerprints, iris scans, and facial recognition technology to protect against illegal immigration, welfare fraud, and terrorism, though implementation is at least two years away.

Since ID authentication and financial institutions go hand in hand, U.S. institutions have long been enthusiastic about more reliable identity authentication, especially U.S. drivers' licenses, which are America's de facto national ID cards. But the idea hasn't had much support.

Although 16 states collect some form of biometric data, such as fingerprints or facial-recognition parameters for in-house databases, only Kentucky has biometrics on the license itself. Kentucky's license reduces a driver's face-recognition parameters--various facial measurements--to a bar code that can be read only by a pre-programmed reader at the state department of motor vehicles. Financial institutions may also choose to buy them.

This year, 14 states had bills related to biometrics and drivers' licenses. Many of these bills died, however, due to the efforts of the American Civil Liberties Union (ACLU), which says any database of consumers' fingerprints is a privacy violation. "There's no question there are strong bureaucratic rationales for tracking individuals and creating databases, but all too often those looking to do these things look at one side of the issue--what we have to gain bureaucratically--rather than what we have to lose," says Jay Stanley, a spokesman for the ACLU's Technology and Liberty Program. "We have a long tradition of privacy and being left alone by the government in this country."

The ACLU also has protested use of a national ID card, even though proponents argue it would better protect consumers' privacy by moving them away from using social security numbers for identification. But the pendulum of public opinion has been decidedly moving toward national security and away from individuals' privacy concerns, especially since the Sept. 11 terrorist attacks. A recent public opinion poll found 87% in favor of using biometrics to prevent tampering and counterfeiting. And it's becoming difficult to turn the clock back: Already on file across the U.S. are an estimated 250 million to 300 million facial images collected by motor vehicle departments and between 50 million and 100 million fingerprints taken by law enforcement and government officials for a wide variety of entitlement programs.

About the Author

Karen Krebsbach
Writer
Bank Technology
News

This article has been provided to you by *The Point for Credit Union Research and Advice*. If you would like to see more articles related to this topic or other information, visit thepoint.cuna.org for a FREE 30 day trial subscription to *The Point*.