

DIGITAL TRANSACTIONS

Trends in the Electronic Exchange of Value

Momentum for Mobile Money



From contactless payment to mobile banking to P2P, the promise of moving money by wireless handset is finally starting to ring true for processors, merchants, and banks. There's still some static here, though.

PSKRT STD
US POSTAGE PAID
ST JOSEPH MI
PERMIT NO 105

ALSO IN THIS ISSUE:

- PayPal's Virtual Debit Card
- More Tension over Interchange
- ACH: On the Web, at the POS
- BankServ's Multimarket Play

Major handset manufacturers, with the help of innovative technology providers, are now developing voice-print security solutions expected to reach the market this year.

Why You Should Feel Secure About Biometrics

Doubts about the security of biometrics become less relevant as the technology takes its place in new multifactor authentication systems and a secure, universal device emerges to replace wallets, PINs, and passwords, argues Chris Shepler.

Hi, my name is Werner Brandes. My voice is my passport. Verify me.”

The 1992 film *Sneakers* single-handedly set voice biometrics back a good 10 years by perpetuating the myth that a user’s voice could be successfully recorded and played back into an access panel. Indeed, countless spy movies and television crime dramas have depicted scenes of an agent creating a mold from a lifted fingerprint to fool the system.

Hollywood magic can create an array of such fantasies, but when a respected payments-industry veteran such as Biff Matthews raises questions about biometric security, as he did recently in this space (“Why I’m Feeling Insecure About Biometrics,” September, 2006), serious readers take notice.

Matthews admits that his perception of biometric security is based largely on a 10-year-old study that claimed many methods “could all be readily duplicated.” The reality is that not only has biometric technology improved significantly in the last 10 years, but also certain methods offer greater advantages over traditional forms of user authentication.

For the record, the biometric market will reach \$7 billion by 2008, according to ABI Research. The fingerprint payment system Matthews describes in his article now boasts 2,200 locations and 3 million users. His favorite method, signature dynamics, is the fastest-growing of all the major biometrics (although off a very small base). And, most important, the convenient multipurpose device Matthews is looking

for has, in fact, arrived.

The success of biometrics is being driven largely by the failure of existing security systems based solely on secret knowledge, such as a password, PIN, or Social Security number. Such information can easily be disclosed, lost, forgotten, stolen, phished, pharmed, or hacked, leading to \$47 billion in identity theft, and millions more in password resets.

By contrast, biometrics—the measurement of a unique physical characteristic of each individual user—provide an added layer of security not susceptible to these threats.

Biometrics are generally divided into two categories: behavioral and physiological. Most biometrics are physiological, including finger, iris, retina, and face. Behavioral methods, which measure the unique way an activity is performed by the user, include signature, gait (walking), and keystroke. In fact, the latest implementations of voice are both behavioral and physiological, as the system measures how the person speaks a certain phrase, while simultaneously using tell-tale features of the speech to determine the size and shape of the speaker’s vocal tract.

Not As Seen on TV

Like PINs and passwords, biometric credentials are often stored in a centralized database. It is this component that stimulates initial concerns about biometrics, relative to the risk of a database being hacked. When a thief obtains a list of passwords, the results are devastating. However, such is not the case with biometrics.



Chris Shepler is co-founder and chief financial officer of Porticus Technology. Prior to founding Porticus, he worked for more than a decade in the financial-services industry. Reach him at cshepler@porticusinc.com.

A stored voice print, for example, is a string of data that is meaningless without the proprietary algorithm that created it. The voice print cannot be fed into the system in any way to gain access, nor can it be used to re-create the original voice. In this way, biometrics solve the common problem of hacking and mass disclosure of log-in credentials, both of which are highlighted all too frequently in the news.

Duplicating biometrics is not as easy as it appears on TV. For example, in *Sneakers*, the hackers had to get a microphone close enough to character Werner Brandes and convince him to say a particular set of words, which they proceeded to splice together and play back into the voice box. In real life, this approach would have been an utter failure. That's because each time the voice is recorded and played back on successive microphones and speakers, the signal is distorted by the unique resonance of the devices. Even with the highest-quality digital-recording equipment, the analog-to-digital conversion (and back again) affects the signal to a perceptible degree.

Biometrics do not claim to be 100% accurate, given that, by definition, they are measuring analog features that are not always presented in the same fashion. The finger can be greasy or tilted the wrong way, the face can be poorly lit or turned to the side, and eyes can be closed or covered with glasses.

What biometrics **do** offer is a confidence level, or the probability that the subject is in fact who he or she claims to be. Depending on the value of the situation, some applications will accept the user at a 75% confidence level while others require 99.9%. The trade-off for higher security is that sometimes even a legitimate user will be rejected falsely because the setting is so strict.

To improve both security and user experience, some biometric authentication systems combine multiple

factors. In fact, government- and industry-recommended mandates are now directing businesses to employ multifactor authentication, which will ultimately lead to increased biometric deployment to the masses. ATMs today, for example, employ double-factor security combining a card with a PIN.

Multifactor systems can include: a *password* or *pass phrase* (something the user *knows*), a *token* (something the user *has*), and a biometric identifier (something the user *is*). What's more, biometrics can be used to eliminate cards and other expensive and annoying single-use tokens that must be readily available for a transaction to take place.

Universal Device

To be accepted by the mass market, a biometric must be convenient, non-intrusive, and user-friendly. It must not require specialized sensory equipment or be associated with law enforcement. And most of all, it must be universal.

Matthews is seeking a

universal device to replace his keys, wallet, tokens, PINs, and passwords to access physical locations and sensitive information. He is not alone in yearning for this futuristic device. What he may not realize, however, is that he probably already possesses such an appliance—a cell

phone. Mobile handsets today come packaged with a microphone, the ability to run various applications, and a connection to the outside world. Major handset manufacturers, with the help of innovative technology providers, are now developing voice-print security solutions expected to reach the market this year.

Why voice? Voice biometrics are growing in popularity given that speech is the most natural form of human communication. Samples can be collected using common, ubiquitous microphones found in telephones, laptops, and cell phones, making voice verification a software-only solution. That's a critical differentiator for inexpensive deployment and scalability.

With integrated voice biometrics, a standard cell phone can deliver triple-factor security in one transparent step as the user must simultaneously *have* the phone, *know* the phrase, and *be* the voice.

What's more, credentials can be stored on the device, on the server, or split between them.

Consumers now have a convenient solution that will not sacrifice security.

As consumers dream of securely and remotely purchasing something through an m-commerce portal, checking account balances, transferring money to their children at school, unlocking their cars, authorizing a credit check, or entering an office building with confidence, biometrics industry players suggest that everyone stay tuned. **DT**

(Editor's Note: For another take on biometrics, see Security Notes on page 13)

