

Comments to U.S Treasury Department
The Use of Biometrics and Other Similar Technologies to Combat Identity Theft
April 2004

Identity theft is usually defined as the misuse of personal information about someone by an imposter for conducting two types of activities: gaining access to existing accounts that the victim has already established (“account takeover”), and opening new accounts in the victim’s name (“new account openings”). It is important to note that FACTA is not simply directing the Treasury Department to conduct a study on the use of biometrics and other similar technologies for “providing convincing evidence of who actually performed a given financial transaction”, but specifically requests that the study focus on the use of biometrics “to reduce the incidence and costs to society of identity theft.”

1 (a) What range of biometric solutions could the private sector use to reduce the incidence and costs to society of identity theft by providing convincing evidence of who performed a given financial transaction?

According to a survey of identity theft victims performed in July 2003 by the Identity Theft Resource Center, a non-profit group that provides assistance to identity theft victims, the most common form of identity theft involved the misuse of personal information by the thief to open a new credit account in the victim’s name. Seventy three percent (73%) of respondents in the survey reported that new accounts had been opened in their names by imposters. The possibility that a thief can use an individual’s personal information to open new accounts in an individual’s name, and thereby ruin his/her credit rating by leaving the bills unpaid, has been cited by some as one of the most insidious and damaging forms of identity theft. Identity theft involving new account openings can take place in person, or remotely (e.g., over the phone or via the Internet). In either case, it is very likely that the creditor will have had no previous relationship with the person whose identity is being claimed. If there is no previous relationship between the creditor and the person whose identity is asserted in the new account application, then it is very unlikely that the creditor will be able to match a biometric provided by the person opening the account with a stored biometric. This would seem to preclude the use of biometrics for preventing many identity thefts involving new account openings, unless (a) the creditor can determine that the person named in the new account application has a biometric template on record with some trusted third party, and (b) the biometric template can be accessed for identity authentication.

Because the creditor in this case wouldn’t have a biometric template on file for identity authentication purposes, it would be easy to simply eliminate this scenario from further consideration, and focus instead on how biometrics might prevent identity theft in other situations where the creditor knows the person whose identity is claimed. But because identity theft often occurs when new account applicants are claiming an identity unknown to the creditor, the usefulness of biometrics in preventing identity theft should address this situation. To do so requires an assumption that a biometric presented by a new account applicant can be compared to a biometric template stored by a trusted third party. The

proposed study should therefore address this possibility, and should explore the implications of using trusted third parties for performing biometric identity authentications. For instance, a bank at which someone has an account might store that person's biometric template for identity authentication when accessing his/her accounts. It would be interesting to study whether and how these biometric templates could be accessed and used for remote authentication by another creditor desiring to authenticate someone claiming the same identity as the bank's customer.

In the case of identity theft involving account takeover, the true account owner is known to the creditor who opened the account. Hence this creditor may already have a biometric template of the true owner on file that could be used for identity authentication. For in-person attempts at account takeover, or in-person attempts to open a new account with a creditor who already knows the person whose identity is claimed, the use of biometrics to authenticate the applicant would be the most straightforward. For remote attempts at account takeover, even if the creditor has a biometric template on file, any use of biometrics for authentication would need to ensure that the biometric presented by the remote claimant is "live", and not a copy. This would increase the expense and complexity of using biometrics in this situation.

1 (e) Does the private sector have adequate incentives to adopt biometric and other technologies to reduce the costs and incidence of identity theft?

In today's environment, most creditors perform very little, if any, identity authentications when processing new account applications. Legally, they are not liable for damages to identity theft victims if they mistakenly open a new account for an imposter. Rather than taking the trouble to perform adequate identity verifications when new accounts are being opened, it is often more convenient for creditors to write off the losses (and pass them on to consumers) when fraud occurs. One way to create greater incentives for creditors to better authenticate the identities of those opening new accounts might be to limit immunity from liability in identity theft cases only if the creditor can demonstrate that a good faith effort was made to verify the identity of the account applicant. Until this happens, it seems unlikely that there will be much incentive for widespread use of any authentication technologies (including biometrics) for preventing fraudulent account openings, especially when the creditor does not know the person whose identity is being claimed.

8. What barriers are there to the greater use of biometric and other technologies to reduce the cost and incidence of identity theft?

Someone attempting to open a new account, or to access an existing account, may do so in-person, or remotely (over the phone or online). The big difference between the in-person and the remote case is that when the biometric is presented remotely, it is not clear that the biometric is actually being supplied by person whose identity needs to be authenticated. It could instead be a copy or recording of someone else's biometric. This problem does not

exist with an in-person appearance. Hence, any usage of biometrics for remote identity authentication needs to consider the “liveness” factor; that is, is the biometric “live” or is it a copy? This would seem to limit the range of biometrics that might be economically applicable in a remote setting. For instance, for online financial transactions, it might seem that fingerprints might be an appropriate biometric, since finger scanners can be connected to home PCs. However, the downside is that finger scanners are expensive, especially those that purport to measure “liveness” factors such as skin conductance or blood flow. On the other hand, the use of voiceprints in remote settings not only requires no special equipment (other than a microphone), but liveness can easily be determined by conducting a query/response interaction with the subject. However, other factors (such as background noise) may lead to reduced performance.

Bob Pinheiro
Independent Consultant