Biometrics: Technology & Policy Webinar Q&A*

*The opinions presented in the answers to these questions submitted as part of the webinar are those of Mr. Lott and Mr. Loudermilk and do not necessarily reflect those of the Federal Reserve Bank of Atlanta or the Federal Reserve Board of Governors.

1. **How does biometric identification on a cell phone compare to a dedicated biometric system?**
   This is difficult to answer without more specificity as to the exact parameters of the devices being compared. Apple claims that the false-positive rate for its fingerprint reader is 1:46,000 whereas its facial recognition false positive rate is 1: 1 million, except that identical twins and siblings who resemble a parent have a lower rate. If by "dedicated biometric system," you mean a commercial system for, say, access control, such systems should have a higher threshold since the enrollment of an individual and the capture of the relevant biometric is under a more controlled environment and the biometric reader devices (camera, fingerprint scanner) are more sophisticated (and expensive). Fingerprint sensors used on cell phones have, to date, had far smaller (typically ¼ inch) sensors than are otherwise used. Thus, there is much less information available for matching. NIST examined this issue for the FBI in 2014 (NISTIR 7950) and found two-finger miss rates ranging from 55 percent to 97 percent, although false-acceptance rates were good. Single-finger matching, as is done on cell phones, was not examined but certainly would had been worse. These small sensors are effective for single-person authentication to a personally owned and controlled device, but are in no way comparable to conventional technology. Cell phone cameras, on the other hand, are high-resolution devices. Today's mobile camera optics are good although not comparable to SLR or even point-and-shoot cameras. However, the algorithms used within cell phones are not comparable to top-of-the-line algorithms used in dedicated systems. If they were, all other factors being equal, we would see comparable performance. Most mobile use cases are not able to control comparably for pose, expression, and illumination issues. However, if the cell phone were used for image capture only and the actual matching were to occur on the dedicated system and appropriate efforts were made to comply with International Civil Aviation Organization, visa, passport, or mugshot image guidelines, you would expect the usual dedicated system results.

2. **How do you expect the criticism of "algorithm bias" and the pandemic to impact the market for biometric identification?**
   We discussed in the webinar how facial masks have created problems for facial recognition programs. They substantially downgrade the matching capability. We also discussed the academic and media stories about alleged bias of some of the facial recognition algorithms. As the NIST evaluation noted, of the 200-plus algorithms tested, the top performers exhibited no evidence of bias whereas the poor performers did have significant matching-rate variations among different ethnic and gender groups. One possible explanation for the poor performance of some of the algorithms is a small database used to "train" the algorithm.

3. **You mentioned the issue with COVID masks for facial recognition. Any near-term solutions?**
   While vendors are working to improve the reliability of their facial recognition algorithms using only the visible parts of the face, when you block off one-half to two-thirds of the surface area, it is going to create major challenges. As we noted in the discussion, efforts are concentrating on the periocular region (area around the eyes), and we're seeing

improvements. The best performing pre-pandemic algorithms had about a 5 percent performance impact, which is better than we could have reasonably expected. Significant improvement is expected as algorithms are tuned to work with both masks and maskless probes. It is unrealistic to expect that performance against masked probe images will be as good as when maskless probes are presented.

4. **Can you describe the differences between data security and authentication?**

   Both of these are somewhat general terms with a broad range of potential meaning. Generally, data security is the protection of information from unauthorized access or corruption throughout its entire lifecycle. Authentication is a process of proving an individual's identity.

5. **Since banks are required by regulations to protect their consumer customers, why are consumers concerned about their safety when using bank services?**

   One could argue that many consumers do not exhibit a high level of concern, as evidenced by poor data security practices such as easily guessed passwords used across multiple online accounts. There is also the thought that consumers expect that their financial institution has a sufficient level of defenses and fraud controls to prevent unauthorized access to their account. On the other hand, consumer research conducted by the Federal Reserve and other research firms has consistently shown that "security" is a major concern of consumers when either using electronic banking products or serving as a barrier to the use of those products or services.

   Many millions of persons have had their data, including financial data, that had been entrusted to government agencies, financial institutions, and retail organizations hacked or otherwise improperly disclosed. Consumers do not reflexively extend trust to bank stewardship when they have otherwise found that trust to be undeserved with others they've entrusted with their information.

6. **What could be done to recover a biometric database that has been compromised? Can that biometric ever be used again anywhere?**

   If the original enrollment images, as opposed to the extracted templates actually used in matching, were compromised, a combination of human observation and liveness checks would be required to prevent matching. This situation would be complex to exploit as the attacker would need to know that a subject was enrolled in both systems to exploit it, and then would need sophisticated technology and knowledge to develop spoofs to circumvent quality sensors. The complexity of the problem very much depends upon the biometric modality used. Fingerprint, face, and iris systems can all be attacked but high-end systems are difficult to spoof for all modalities. Today, many sensors and systems do include liveness detection. If and when this becomes a problem of more than theoretical interest, it is expected that all systems will incorporate liveness checks. The technology for presentation attack detection is rapidly advancing due to government-sponsored research, which is largely being shared in the open literature. Market-leading biometrics vendors are producing only sensors that incorporate presentation attack checks. Also, certification programs now exist for presentation attack or spoof detection and vendors are seeking and slowly obtaining certification.

In the more realistic case that the file of templates is compromised, a presentation attack would still be difficult to construct that could not be detected by an observer or automated liveness detection. But even if that attached were undetected, it would only be effective against another system from the same supplier and at the same release level.

7. **Your definitions are different from industry jargon—false positives occur when a good customer is rejected.**

   No, our definition on slide #19 is correct. A false positive occurs when images of two different individuals are incorrectly scored as being the same individual. A false negative takes place when images of the same individual are scored as being two different individuals.

8. **How long will it be before biometrics are made part of the card-present and card-not-present transaction set? It took 20 years or more before chip cards and EMV showed up in the infrastructure.**

   As with any fraud defense tool, it is a matter of economics. There are payment cards in the market today with biometric fingerprint capability, but they are quite expensive to produce and have had minimal issuance. As far as the CNP environment, some of the payment methods (such as ApplePay) available to e-commerce merchants incorporate a biometric authentication of the device owner to complete the transaction, although such authentication does not necessarily mean that the individual is authorized to use that particular payment method. As we stated in the webinar, biometrics are but one of several tools that can be used in the authentication and authorization of a payment transaction and the more tools that are used, the higher confidence in the legitimacy of the transaction.

9. **Is there any movement in the payments industry or mobile-service-provider industry to adopt a single biometric standard?**

   Not to our knowledge. Neither a single biometric modality nor a particular national or industry standard for a particular modality has captured universal support.

10. **Do you think biometrics should be used to validate a consumer in a card-not-present payment transaction to reduce fraud and false declines, which continue to grow online?**

    See the answer to #8 above.

11. **Should the payments networks allow time in the authorization process for a consumer to respond providing a biometric to a mobile device?**

    Strictly a personal opinion: NO! The efficiency of the payment card authorization system in the United States with 99 percent online authorizations is based on authorization decisions being made in milliseconds, not minutes. A number of payment card providers offer alert services whereby a text message is sent to the cardholder advising them of a card transaction. In some cases, the cardholder can customize such alerts with filters to limit the notifications to transactions having a higher risk such as card-not-present, international, or above a specified dollar amount.