

Biometric Caller Verification: Top 10 Reasons Why You Need To Implement It Now

Written by Haim Argaman

Crimsonet Technologies, Inc.

December 2009

crimsonet
Driving Voice Recognition Success



Caller authentication is a fundamental part of proper privacy best practices and fraud prevention. It can take different forms, from simple question-and-answer by an agent, to automated caller verification using voice biometric technology. Biometric caller verification is increasingly common in the call center industry, and a crucial step towards enhanced call center security. With biometric caller verification, a caller's unique voice profile is used to confirm his or her identity. Voice biometrics uses information such as the pitch, tone, and rhythm of a caller's speech to authenticate him or her. In addition, the biometrics solution would verify the caller's answers to cross check the identity of the caller – all in a very short period of time.

Why implement it now?

- 1) **Recent increase in rate of identity theft** - Identity theft is a growing problem in all markets. The 2009 report of Javelin Strategy and Research Center estimates a 22% annual increase in recent identity theft rates.¹ Biometric caller verification may assist in reducing its growth rate, as it makes it incredibly difficult to impersonate a caller.
- 2) **Introduction of high-level regulatory standards** - Regulatory standards have upped the demand for privacy enforcement, particularly in financial institutions where the costs of fraud can be devastating. Regulations such as the HIPAA, SOX, GLBA, and the recent ISO 19092 define a framework for implementing advanced caller authentication procedures in organizations.
- 3) **Experience shortened call times** - Biometric caller authentication minimizes the time a caller spends on a call. Instead of taking the time to answer security questions or fumble for a password, callers can go straight to getting their needs met. This ensures a higher level of caller satisfaction.
- 4) **Achieve enhanced user experience** – Biometric voice authentication provides a quality user experience compared with many other procedures. Many currently used authentication procedures, such as the use of passwords or question-and-answer dialogues, may lead to a poor user experience. Taking the time to answer a string of security questions, or having to zero out to an agent because of a forgotten password, can contribute to a negative caller experience and leave a bad taste in the caller's mouth.
- 5) **More effective security is needed** - Common authentication procedures are not as secure as biometric caller authentication. If a password is apprehended, or if the answers to security questions are known, then anyone can impersonate a caller. How many times have you been asked your mother's maiden name? Consider how simple it would be for someone to track down this information.
- 6) **Gain greater cost savings** - Current authentication procedures are very costly. Especially if a caller has to speak to an agent, the call can cost anywhere from \$12 to \$15. With self-service biometric caller authentication, the cost of a call can be well under \$1.² Organizations such as TD Waterhouse, Bell Canada, ABN Amro, National Australia Bank, and Aeroplan have already seen major benefits from using biometric caller authentication.

¹ <http://www.spendonlife.com/guide/2009-identity-theft-statistics>

² http://www.internetevolution.com/author.asp?section_id=679&doc_id=181166&f_src=internetevolution_gnews

7) **Get faster and easier deployment** - Deployment of biometric caller authentication is easy and fast, as it does not require major changes in an existing IVR infrastructure. The biometric authentication module can easily be added to any existing IVR implementation, and the change needed to the existing script is minimal.

8) **Have platform-independent authentication** - Biometric caller authentication supports the use of person verification through multiple media, including via phone and online. For biometric caller authentication, there is no need for specific hardware, other than a phone or microphone for online transactions. Biometric caller authentication is not invasive and is natural for the call.

9) **Minimize false rejection rate** - The rate of false rejection with biometric caller authentication is virtually none. Should a caller fail the authentication test, it is likely that they are in a poor environment with heavy noise pollution. In this case, callers will be automatically transferred to an agent to be manually authenticated.

10) **Lower implementation costs** - There is a low cost of implementation with biometric caller authentication. Nowadays, businesses do not necessarily need an initial up-front investment to license technology. After investing in initial application deployment, a business can pay based on the level of transactions. With hosted solutions, deployment costs are particularly low.

Now is the time to implement biometric caller authentication!

Biometric caller authentication is growing more and more common in call centers. For companies requiring a high level of security, such as financial or medical institutions, the importance of caller authentication cannot be underestimated. As more call centers move towards biometric caller authentication, it is an increasingly inadvisable practice to remain with traditional and less secure authentication measures.

Giving callers the option of choosing biometric caller authentication is one way to verify its popularity with clients. In fact, firms which instate voice-based verification find that the majority of callers choose to enrol and register their voice stamp. If there is any further doubt as to this burgeoning trend, the market revenue for biometric caller authentication solutions is projected to grow to \$800 million by 2011.³

The benefits of biometric caller authentication are lower call center operational costs, improved caller satisfaction rates, and of course, heightened security. With fewer fraud cases to address, call centers can focus on providing the best possible caller experience and increasing business profitability.

Best practices to implement biometric caller authentication

1) Strategize and plan ahead

To maximize the effectiveness and profitability of an IVR system update, it is crucial to have a clear road map. Implementing biometric caller authentication is no different. Ask yourself, what is the objective of a new authentication procedure? Who are the callers who would undergo biometric caller authentication? How will biometric caller authentication be integrated into the system? How will callers be transitioned to the new security procedures? Answers to these questions will depend on a multitude of

³ http://opusresearch.net/wordpress/pdfreports/vbio_mktpntnl_leadup.pdf p. ii

factors, and affect the successful implementation of biometric caller authentication. Bearing in mind that caller responses cannot be predicted with 100% accuracy, it is also important to monitor key metrics so that adjustments can be made accordingly.

2) Deploy voice biometrics

When deploying any change to a call center's IVR system, it is important to ensure that callers are prepared for the change. Give callers time to record their voice stamp, and alert your client base of the security change via as many channels as possible (email newsletters, mail invoices, website updates, and so on).

3) Monitor key metrics

Monitor and tune changes over time to ensure that the IVR system is not disrupted and the functioning is kept smooth. Over time, the caller's database should adhere to the changes that affect the caller's life to ensure the continued accuracy of the biometric caller authentication.

About Crimsonet Technologies

Crimsonet offers IVR and voice recognition software consulting for call centers and businesses through all phases of the IVR development life cycle. The company emphasizes **caller experience** and the importance of **secure authentication** as a means for inspiring trust and diminishing call center fraud. With a focus on developing biometric caller authentication, Crimsonet creates IVR systems that are **secure** and **user-friendly**.

As part of the company's strategy, Crimsonet features a strong orientation towards financial and business goals. Crimsonet regards every voice recognition project above all as a business investment, gearing IVR projects towards specific company goals. High-level experience in telecommunications and software development allow Crimsonet to translate these company goals into system requirements, whether for caller authentication, self-service functions, or for IVR script development. Ultimately, Crimsonet's orientation towards business needs guarantees higher returns and a more worthwhile company investment.

Crimsonet follows a careful procedure for IVR development. Beginning with ROI analysis, Crimsonet creates business models that maximize project returns and minimize risk. Subsequent strategic planning and project scoping create a game plan for the application development and deployment of IVR systems. In addition, Crimsonet leads system testing and tuning for optimal functioning, and finally sets up a post-deployment monitoring system to guarantee continued efficiency. From beginning to end, Crimsonet aims to make speech recognition projects a success. Ultimately, Crimsonet's orientation towards business needs guarantees higher returns and a more worthwhile company investment for clients.

For more information on biometric caller authentication and Crimsonet's other IVR system consulting services, visit the Crimsonet website at <http://www.crimsonet.com> or the company blog at <http://www.crimsonet.com/speech-recognition-blog.html>. Read Crimsonet's white paper on "How ROI Analysis Can See Your Company Through the Economic Downturn" at <http://www.crimsonet.com/voice-recognition-white-paper.html>.