



## Making Sense of a Biometrics Portfolio in an M&A Strategy

---

By John Checco, Director & John Stroud, Managing Director with Iris Capital Partners

Most of us know the concept of “biometrics” but few decision makers understand the business of biometrics and how it can play a role in an M&A strategy to enhance a company’s business portfolio and foster growth.

Taking the steps to understanding the business of biometrics is to dispel any preconceived notions about biometric technologies, recognize the timing for expansive growth in this market, comprehend the business drivers that influence biometrics technologies, and identify causalities for biometrics in a thoughtful and creative M&A strategy.

### Perception of Biometrics

Biometric technologies have some interesting myths surrounding them. For many people, the idea of fingerprint devices garners visions of Big Brother in “1984”; although most devices store data in proprietary formats – only specific areas of the government use the AFIS format that generally concerns the public.

Commensurate with this concern is the perception that biometrics are intrusive. Although this is visibly so with physical biometrics such as fingerprints and iris scans; behavioral biometrics such as handwriting signature verification, voice recognition and keystroke dynamics measures the characteristics of what users normally do. For behavioral biometrics, the least intrusive workflows provide better validation.

Also high on the myth list is the notion that biometrics are infallible. Tsutomu Matsumoto, a Japanese cryptographer, compromised eleven commercial fingerprint systems with about US\$10 of household supplies. One rule of security is that nothing is infallible (Rule #1: Not “if” but “when”).

From a technology standpoint, biometrics are seen as absolute technologies – either you pass or fail. This is only true for physical biometric technologies which match explicit points of distinction. Behavioral biometric technologies return “confidence” measurements which, by design, have the benefit of allowing for varying levels of risk mitigation.

Finally, there is the myth that biometric security needs to be perfect. Perfection is ideal, but assuming technology is perfect leads to a false sense of security. A company deploying any security technology needs to plan for false positives as well as false negatives (Rule #2: Defense in Depth).

## Acceptance of Biometrics

Although a lack of understanding has played a small factor in the slow adoption of these technologies, the real issues have centered on placement and timing challenges.

Once touted as the demise of passwords and keys, biometrics should never be used as a single authentication mechanism; it is only in the last decade that companies have realized that it should exist only as one part of a multi-factor authentication and verification model.

And it wasn't until the last decade that enterprises (outside of government) started in earnest the process of "data classification" to protect their intellectual property. This revelation was born out of the internet explosion of access to a plethora of worldwide data. Prior to this milestone, biometrics had very few items to protect that warranted its expense.

Now, in the age of ubiquitous information exchange and mature security principles, biometrics has increased in the breadth of technologies offered and decreased in deployment complexity and costs.

## Biometric Drivers

Understanding the basic principles of security design allows one to plan accordingly on how specific biometric technologies can best be utilized. There are three business drivers for considering a biometric strategy: regulation, retention or differentiation.

Government Regulations are the most effective driver for many companies to minimize liabilities. The FTC stated that financial institutions "implement reasonable physical, technical, and procedural safeguards to protect customer information."<sup>1</sup> And the FFIEC<sup>2</sup> "Authentication in an Internet Banking Environment" Guidance of 2005 is more specific, recommending that all financial institutions have multi-factor authentication for internet-based services.

Companies that consider biometrics for compliance see it simply as the "cost of doing business". These companies are likely to spend the least amount of capital and operating budget on a biometric technology.

Customer Retention – loss prevention due to inadequate PII (personally identifiable information) protection is a more business-driven factor for implementing multi-factor security. Outside of the infamous incidents of TJX (130MM records), Heartland Payment Systems (94MM), TRW Sears Roebuck (90MM) and the National Archives and Records Administration (76MM); there have been 438 reported

data breach incidents in 2009 alone resulting in 219,256,849 PII records being compromised.<sup>3</sup> Companies that fail to understand the rippling effects of poor decisions about the safety and security of its customer base – Toyota being the most recent example of this – are destined for long-term ramifications.

Companies that deploy biometrics as part of their existing product/service view the costs as “risk mitigation” or “loss prevention” items. While no added revenue is generated from implementing biometrics in these situations, the companies do recognize the importance of “security theatre” – ensuring their customers are confident in their efforts. These companies will spend more money on biometric technologies that are visible, yet usable (and cost effective).

Product/Service Differentiation should be the most compelling driver for considering biometrics. Biometrics, offers three distinct verification models for product/service enhancements: independent, mitigated and augmented.

*Independent verification* of an existing product or service means that the biometric solution provides verification analysis and results which are used to wholly confirm or deny a primary authentication. Independent biometric verification results can be considered forensic evidence in some litigation.

*Mitigated verification*, unique to behavioral biometrics, allows the behavioral confidence measurement of the secondary verification to determine dynamic access levels. For example, several financial institutions implementing keystroke dynamics have thresholds that determine whether a confidence measurement for a particular user login will allow them read-only access, intra-bank transactions or full account access and transactions. This leads to a better user experience, and also plays a role in customer retention.

*Augmented verification*, also unique to behavioral biometrics, specifies that a primary authentication result is accurate to within a certain percentage. While this initially does not seem like an attractive alternative, it’s value become apparent when a company can state that their product has a level of verification at a specific percentage higher than its rivals.

Companies that integrate biometrics into their products and services to increase revenue are motivated by both high levels of security theatre as well as usability. These companies are willing to spend larger amounts for biometric solutions if the ROI can be proven within a reasonable timeframe.

## **M&A Considerations**

Understanding the operating landscape of the biometrics industry affords us to look at the unique opportunities that exist in complementing an M&A strategy with the right biometric technology company.

### **... For Non-Biometric Companies**

There are several reasons for enterprises to pursue an M&A strategy involving biometric companies.

The first is to acquire a technology that uniquely bolsters the “Value Add” of an existing product and/or service. As a manufacturer of access keypads pointed out, “If our keypad with biometrics is only 10% more effective than our competitor’s without biometrics, we’ll get the sale.”

The second approach is to acquire technologies that bring new audiences to your brand and add another technology that you can resell to your existing customer base.

The third approach is to use the acquisition of a biometrics company to round out an M&A portfolio that is in need of a cutting edge technology base. The use of such an acquisition is not isolated to reselling the company’s products. In the 1980’s, IBM’s Research division hired as many musicians and free-thinkers as it did post-doctorates. Today, many hedge funds and financial institutions make heavy use of the same techniques used by biometric technologies: predictive analysis, quantitative analysis and derivatives.

### **... For Biometric Companies**

For the biometric technology company, a pre-meditated M&A strategy represents maturity in business planning. John Stroud, in a white paper published by Iris Capital Partners, outlined the benefits of “growth by acquisition”. Not only can an acquisition reduce operating costs by consolidating sales and marketing efforts, it can allow for growth by inherently opening the biometric company to a larger existing customer base and new markets or revenue streams.

An acquisition strategy can be used to attain funding for research that keeps the biometric company ahead of its competitors. Or it can be used, as in the case of CA’s acquisition of Netegrity, to redefine the direction of the technology in a way that could never be accomplished through organic growth alone.

Finally, today’s economic climate will force many small-to-medium size companies to merge to create the size and stability necessary to persevere. Consolidation is no different for the lifecycle of any industry – expansive growth followed by competitive paring, consolidation and stability. Biometrics, or information security as an industry, is on the cusp of such a consolidation curve.

## **Conclusion**

Adding the right biometrics technologies to an M&A portfolio has multi-faceted benefits; from market expansion and revenue generation to strategic direction and increased branding opportunities. Comprehending the business of biometrics to complement one’s existing knowledge and focusing on the proper goals are the keys to leveraging this technology for the benefit of your business.

## **About Iris Capital Partners**

Iris Capital is a boutique, independent advisory firm with locations in Washington, DC and New York, NY specializing in corporate development, investment banking and mergers & acquisitions services. Our clients include government contractor and privately held companies in information technology, fossil fuel and alternative energy, cyber security, professional services and advanced analytics, who are interested in growing, restructuring or selling their business.

For more information, please visit us at [www.iriscappartners.com](http://www.iriscappartners.com) or contact us by email at: [info@iriscappartners.com](mailto:info@iriscappartners.com) or by phone at + 1 202-521-4440 ext 107.

---

<sup>1</sup> Source: “FTC Testifies on Data Security and Identity Theft” (<http://www.ftc.gov/opa/2005/06/datasectest.htm>)

<sup>2</sup> FFIEC (Federal Financial Institutions Examination Council) is comprised of the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

<sup>3</sup> Source: <http://datalosssdb.org/reports>