

BUSINESS CASE

IDENTITY DATABASE DE-DUPLICATION SERVICE

EFFECTIVE IDENTITY RESOLUTION SERVICES AS A MEANS TO MINIMIZE
IDENTITY FRAUD AND MAXIMIZE AGENCY RESOURCES

merkatum
Biometric ID Management



IDENTITY DATABASE DE-DUPLICATION SERVICES

BUSINESS CASE - EFFECTIVE IDENTITY RESOLUTION SERVICES AS A MEANS TO MINIMIZE IDENTITY FRAUD AND MAXIMIZE AGENCY RESOURCES

Challenge – Discovering Identity Fraud in Large Databases

Government agencies, banking institutions, healthcare organizations, and corporations worldwide require to monitor and to maintain an updated and error-free database of their existing customers, patients, civilians, and/or employees in order to provide better service, generate more income, and reduce costs.

Some examples of these types of identity-centric databases include:

Banks and Insurance	Passports and Driver Licenses
Healthcare Providers	Public Safety and Justice
Government Social Benefits	Electoral – Voting
Revenue and Tax Collection	Energy and Telecommunications

There exists a huge underlying value of the services and benefits provided to individuals registered in these databases (such as salaries, medical benefits, etc.). Thus, it is necessary to continuously monitor and supervise the security, access rights, and composition of these databases.

Opportunity – The Identity Resolution Approach

Consistently, these identity-centric databases are “contaminated” by multiple representations of the same individual (manifested as duplicate records of the same person) due to deliberate identity-fraud instances or by data-entry errors or omissions in the enrollment process.

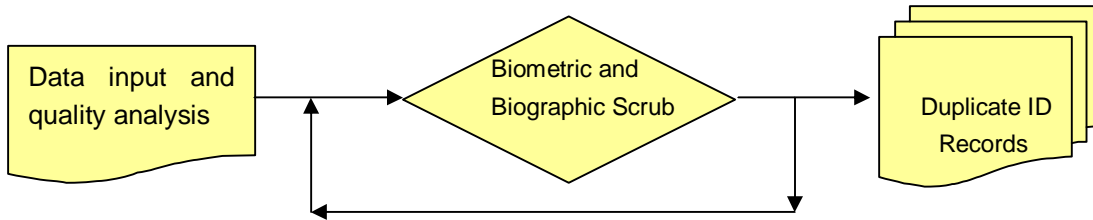
The underlying value of “de-duplicating” or “sanitizing” these databases, *at an identity level*, above and beyond tactical savings on computing equipment, software licensing, and storage resources, implies the capacity to unleash tremendous economic value by discovering and addressing opportunities where system security or fraud-related loopholes exist.

Solution

Identity De-Duplication

The process requires validation that the target database is clean and non-redundant, from an identity perspective. An “Identity De-Duplication Process” is performed to identify repeated records assisted by advanced biometric (e.g. facial, fingerprint, signature, etc.) recognition and biographic (key entry, phonetic, name recognition) authentication algorithms.

Process



- ✚ The identity de-duplication process involves comparing all records of the target database among them, powered by complex mathematical algorithms that discover physiologic and/or demographic similarity relationships within datasets.
- ✚ Target database records include the demographic profile of the recipient (name, gender, DOB, address, etc.) plus a picture and/or fingerprint image of such person.
- ✚ After the cross-comparison process, duplicate identity records are flagged when the biometric and/biographic determinants of two records are very similar between them.
- ✚ These records are identified as conflictive (multiple records pointing to the same individual) and require a post-processing “cleansing” process either by an offline identity audit procedure and/or by specific database correction activities.

Economics: High-Level ROI Analysis

Business Case: Payroll Fraud - Identity Database De-Duplication Service

- (1) **Volumetrics:** 22,000 contractors in large government agency are paid \$2,000/month for temporary work. Suspicion that certain people are committing payroll fraud.
- (2) **Enrolled Data:** Each employee was issued a photo ID card validated vs. driver license
- (3) **Process:** ID data de-duplication (face+biographics) finds 3.5% of duplicate ID records
- (4) **Solution Investment:** Turnkey De-dup Service > \$1.8 MM, Field Compliance: \$0.4 MM
- (5) **Savings:** \$18.5 million per year in direct compensation costs
- (6) **Return on Investment:** 740% per yr.; Payback: 43 days, Implementation time: 90 days

THE SERVICE: EMFIVA F/FRS® IDENTITY RESOLUTION SERVICE

Merkatum's emfiva F/FRS® is a robust, modular, scalable, and flexible biometric and biographic resolution and identity management platform, provided either as-a-service or "out-of-a-box", that utilizes multi-biometric technology (fingerprint, facial, iris) and textual algorithms (name recognition, phonetic, keystroke, etc.) as a means to physiologically and biographically determining the identity of an individual or data duplicity among records sets. Furthermore, it permits the end-user to enable, manage, and/or control the activities of such individuals as they intend to interact with other people, physical assets and/or information systems.

The emfiva F/FRS® appliance is plug-and-play, simple to use and affordable, thus reducing technological complexities and heightened project implementation costs. It can be configured for different vertical segments including: civil identification, law enforcement and justice, healthcare, banking, and benefits management, among others.

Key benefits associated to the proper implementation of an emfiva F/FRS® -based solution include: risk mitigation, security control, fraud detection and prevention, operational costs reduction, and labor productivity increases.

ABOUT MERKATUM CORPORATION

Merkatum Corporation (www.merkatum.com) develops biometric and biographic identity resolution systems that effectively determine, interpret, and manage the identity of individuals in order to deter identity fraud and safety/security risks. Merkatum's core product, its patent-pending **emfiva F/FRS®** biometric resolution and identity management system, searches and compares the identity of individuals in databases and on the field by utilizing fingerprint, facial, and/or biographic recognition algorithms leveraged by an open, scalable, and business process driven, service-oriented architecture (SOA).

The Company provides transaction-based identity resolution managed services, including ID database de-duplication and enrollment) for high-volume operational environments for specific vertical markets. Furthermore, our Company's objective is to develop and market modular, "out-of-the-box" systems that are easy to install-deploy-maintain at a lower total cost of ownership by pre-configuring and deploying emfiva F/FRS® servers for determined vertical market segments. Merkatum also develops and markets modularized identity enrollment kits ("Eagle Kit") comprised of integrated biometric capture devices (fingerprint, facial, iris, and signature) and data encoders (barcode, document scanners) for military, public safety, and civil identification applications.

The Company has successfully deployed our products and services for relevant customers and high-profiled projects over the past 10 years. Merkatum's target customers include government agencies, healthcare payers and providers, financial institutions, and enterprises worldwide.