

BUSINESS CASE

INFORMATION FUSION CENTERS

**EFFECTIVE IDENTITY RESOLUTION STRATEGIES TO IMPROVE INTELLIGENCE
GATHERING AND DATA-SHARING & COLLABORATION**

merkatum
Biometric ID Management



BUSINESS CASE: INFORMATION FUSION CENTERS

This business case describes the key challenges and opportunities that information fusion center initiatives face and the role that biometric resolution and identity management systems play in this process.

CHALLENGES

- **Information Aggregation and Preparation:** Information fusion centers consistently gather and process huge amounts of structured and unstructured data from multiple sources, mainly from public safety agencies, judicial court systems, private/consumer feeds, and diverse federal government sources. This data must be methodologically aggregated, cleansed, and condensed in order to prepare it for analysis and intelligence purposes. Data volume and format makes this a very complex process.
- **Analysis and Intelligence:** Source data records must thereafter be processed to find relevant correlations for further analysis and action by public safety personnel. In this environment, an important portion of these records have identity-based relationships within them. Sophisticated algorithms perform link analysis routines among objects and datasets (e.g. name of person, car model, criminal background, societal associations, geographic data, etc.) to generate actionable intelligence. Nonetheless, Question of Identity (QID) cross-relationships of persons in datasets driven by biometric (photographs, fingerprints) and/or biographic (names, addresses, DOB, aliases, etc.) information are seldom performed due to its complexity, randomness, and lack of available system tools and applications.
- **Data Sharing and Collaboration:** Once data associations are executed and actionable intelligence is derived from these activities, the objective is to efficiently and effectively disseminate and share this information among accredited public safety agents. There is a need interconnect these individuals in a flexible and simple manner in order to enhance collaboration, increase intelligence, and ultimately deter crime and improve safety.

SOLUTION

Information fusion centers must continually process vast amounts of data. Such data should be processed and associated utilizing robust techniques and best-of-breed systems to perform such tasks. Identity-related data is seldom cross-referenced in this data gathering and link analysis process. An “identity relationships” module within the fusion center is necessary in order to determine co-dependencies. A flexible, robust, and scalable identity management system is thus suggested as a core application for information fusion centers.

This system, ideally, must be able to:

- Gather identity-related data sources from different feeds and source-types
- Systemically compare biometric and metadata using robust and configurable matching algorithms and fusion engines
- Cross-reference this information for intelligence and de-duplication purposes
- Generate identity-based “Bio-Aliases”, Watch Lists, and Alerts
- Flexible and easy-to-operate in order to promote user collaboration
- Receive field-data from multiple source types and devices
- Interconnect to other fusion centers or similar identity management systems, in real time, to maintain data integrity and relevance

SOLUTION BENEFITS

- (1) **Data-Cleansing:** Identity-related records can be cross-referenced and segmented according to their characteristics in a quick and efficient manner.
- (2) **High-accuracy:** When simultaneously comparing biometric and/or biographic data records of individuals, very high association matching rates are obtained, thus significantly improving QID decision-making procedures.
- (3) **Time-efficiency and Productivity:** Actionable intelligence cycles are significantly reduced via automated and semi-automated data referencing, thus having better information, faster.
- (4) **Data Sharing and Collaboration:** Open, adaptable, and scalable identity management system enables for real-time information sharing and collaboration over federated environments and/or disperse geographies.

THE SYSTEM: EMFIVA F/FRS®

Merkatum's emfiva F/FRS® is a robust, modular, scalable, and flexible biometric and biographic resolution and identity management platform, " 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'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 identity enrollment kits ("Eagle Kit") comprised of integrated biometric capture devices (fingerprint, facial, iris, and signature) and data encoders (barcode, document scanners) contained in ruggedized briefcases for military, public safety, and civil identification applications.

Merkatum has successfully deployed its product for relevant customers and high-profiled projects. Merkatum's target customers include government agencies, healthcare providers, financial institutions, and enterprises worldwide.