

Identity fraud is typically encountered in one of three forms:

- **Cloned ID** – The use of another individual’s identity in order to gain access to that individual’s financial assets or access to a facility that the individual has access to; also referred to as identity theft. ID cloning typically occurs in short intervals as the identity thief wishes to avoid detection from the identity victim. Biometrics make it difficult to clone an another individual, but using an individual’s stolen passport could go undetected without performing the proper analysis.
- **Synthetic ID** – The creation of an entirely new identity which is used to avoid long-term detection. For example, the perpetrator might enroll in a program like Transportation Worker Identification Credential (TWIC) in an attempt to avoid detection while involved in organized criminal activities. The perpetrator’s objectives of creating a synthetic identity are to:
 - Avoid having his/her real identity matched to a watch list
 - Reduce the risk of detection by an identity theft victim.

While industry studies show that about 90% of all identity fraud in the credit card industry is driven from synthetic ID’s, not cloned ID’s, current products and solutions tend to focus on cloned ID’s. This is due to the fact that there is a clear consumer victim in the case of a cloned ID whereas with a synthetic ID there is no one individual that is impacted.

- **Alias ID** – The altering of one’s identity attributes in order to avoid detection. This is less sophisticated than creating an entirely new ID, but it works because most existing systems perform “exact match” searching and therefore miss intentional misspellings, cultural nicknames, name juxtapositions, address modifications, etc. Similarity Search technology can detect the use of an alias by performing non-exact matching, which uses multiple attributes (e.g., Name, Address, Phone, DOB, etc.) to assess the likelihood of a match.

BIOMETRICS AND BIOGRAPHIC IDENTITY ANALYSIS

Fingerprint biometrics are the single most reliable, commercially available and culturally acceptable form of “analytic” for authenticating an identity. Fingerprint biometrics are extremely powerful for use in access control applications (e.g., entering a secured facility) and also provide tremendous value in searching criminal fingerprint files for purposes of a background check, enrollment, or credentialing applications.

However, in terms of managing identity fraud as part of a background check, enrollment, or credentialing application, there are additional forms of analytics and data sets that can be used in conjunction with fingerprint biometrics to greatly improve the management of identity management risks. A biometric will prevent the cloning of an already enrolled individual but would not prevent the use of a synthetic ID during enrollment, significantly reducing the effectiveness of any type of watch list matching or hidden relationship analysis. The right solution incorporates both biometric and biographic identity data to understand the history of that identity. By analyzing biometrics along with internal data and publicly available external data, organizations can more accurately verify if an individual is who they say they are.

GAO REPORT – 03-1147T: COUNTERFEIT IDENTIFICATION AND IDENTIFICATION FRAUD RAISE SECURITY CONCERNS



Undercover agents using phony birth certificates, utility bills, baptismal certificates, and fake ID’s from other states, obtained driver’s licenses in all seven states they visited from July 2002 to July 2003. The agents were also able to obtain social security numbers using phony baptismal and birth certificates.

During the border security investigation in which counterfeit drivers licenses and birth certificates were used to enter the US, border inspectors never questioned the authenticity of the documents, and the investigators had no difficulty entering the country.

The report findings were clear: homeland security is vulnerable to identity fraud, and unless action is taken, individuals who intend to cause harm can easily exploit these vulnerabilities.

THE ID SOLUTION: IRE IDENTITY FRAUD DETECTOR

A combination of biometrics and biographic identity analysis is required to detect ID fraud. As part of a Proof of Concept, Infoglide integrated the Cogent fingerprint matching algorithms with biographic identity resolution. Incorporating public data into the process significantly enhances the ability to detect synthetic, cloned, and alias ID's. Public records contain current and previous addresses, current and previous phone numbers, and other important information. During the screening process, searches are performed across multiple public data providers to identify inconsistencies in identity data (e.g., Michael Ramirez' name but w/ Shane Moore's address) and anomalies in identity data (e.g., Michael Ramirez is 36 but his history suggests he has only had a residence for 5 years and credit for 3 years).

Change status to: Pending Approved Denied

Overall Assessment: Watch List Match

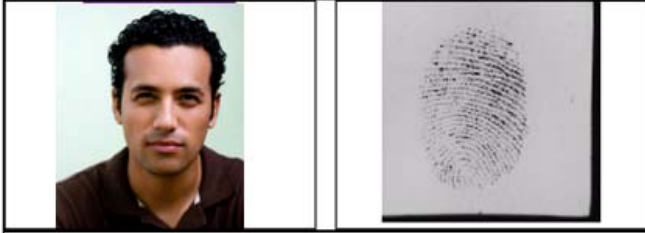
Enrolled Person Checks		
Biometric / Fingerprint		No Match
Biographic		Clear
Phone Number		Clear
ID Validation Check		
Phone Validation		Clear
Address Validation		Valid
Public Records		Near Match
Public Records - Phone		Clear
Watch List Checks		
Watchlist Countries		Clear
NAFIS Biometric Check		Match
FBI Watchlist		Match
TXCASES		Near Match
TXCASES - Alias		Match
Secured Watch List		Match
Criminal Record Check		Clear

ID Verification Questions

Monthly Salary: \$7288

Years at Previous Residence: 2

Biometric Data



Biographic Data

Status		Pending
Record ID	6	
Given Name	Vasten	
Surname	Torrassis	
Nationality	USA	
Passport #	432782982	
Current Address		
Street	405 East 4th Street	
City	Austin	
State/Province	Texas	

A resulting ID Screening Score answers three separate ID fraud questions:

- 1) Is this ID stolen? Has the person in question cloned someone else's identity?
- 2) Do we already know this person or is it a person of interest who is using an alias?
- 3) Has this identity been created? Is it a synthetic ID?

For more information about IRE Identity Fraud Detector contact us at the number below or email us at: IREsales@infoglide.com.

Infoglide Software Corporation
 6500 River Place Blvd., Building II, Suite 101, Austin, Texas 78730
 512.532.3500 • Fax: 512.532.3505 • www.infoglidesoftware.com