Most financial fraud is based on some degree of identification deception, such as posing as another person, but none to the extent of bust-out fraud. The success of both fraud rings and individual fraudsters perpetrating bust-out schemes relies primarily on stealing or synthesizing an identity, and then quickly opening numerous accounts just to “max them out” and disappear. FICO® Identity Resolution Engine is a potent tool to combat bust-out fraud, helping lenders to uncover suspicious links in a person’s identification data across various data sources, as well as suspicious connections between individuals based on shared data attributes.

So, how much money can FICO® Identity Resolution Engine save lenders? According to research, the financial services industry misclassifies between $4 billion and $17 billion as credit loss, rather than fraud loss due to bust-out fraud.

In addition to reducing those losses, Identity Resolution Engine helps institutions protect profitability through greater efficiency; investigators can more quickly and effortlessly identify fraudsters and organized criminal rings, and collections teams spend less time chasing unrecoverable debt.

Lenders’ use of traditional fraud detection models applied during the origination process can help reduce bust-out incidents to a small degree. Now, in addition to these models, lenders are strengthening their detection of bust-out fraud by using Identity Resolution Engine to focus on perpetrators, who leave behind their “fingerprints” of synthetic personal attribute information across numerous data sources.
Why bust-out fraud is different

Unlike the traditional view of application fraud, where most institutions believe they are looking for an individual acting independently, the vast majority of bust-out fraud is committed by organized crime rings. Therefore, bust-out perpetrators go to great lengths to shield their apparent financial integrity and connections.

FICO\textsuperscript{®} Identity Resolution Engine combines federated data search capabilities, identity resolution algorithms, link analysis technology and visualization tools, so lenders can match and link personal attribute information across a variety of data sources. Searching for matches and similarities in addresses, phone numbers, Social Security numbers, driver’s license or personal identification numbers, and many other ID attributes, Identity Resolution Engine helps lenders resolve the authentic or synthetic identity of an individual — “who’s really who” — as well as connections between individuals based on shared attributes — “who knows whom.”

**Data federation speeds investigation**

Identity Resolution Engine is different from other data-matching systems because it uses a federated, cross-database approach to accessing a variety of internal or external data sources. Data federation eliminates the need to build a data warehouse and move data into a separate repository, vastly speeding the preparation of data for analysis. In addition, Identity Resolution Engines uses advanced, proven technology to automate the matching and relationship identity process with extremely high precision and speed.

**Reactive and proactive applications**

Lenders apply Identity Resolution Engine in two ways:

- In reactive mode as an additional risk measure in credit or loan application reviews
- In a proactive mode by analyzing the identities of individuals who are currently account holders.

Used in application screening, Identity Resolution Engine helps issuers significantly reduce fraud by preventing suspicious individuals from opening accounts, and by looking for connections to current accounts from suspects who were denied credit.

**How it works: Five core functions**

Identity Resolution Engine significantly advances fraud investigations to reduce fraud losses, improve workflows and enable greater collections efficiencies.

**Search**

Identity Resolution Engine provides federated access to enterprise and third-party data. It can simultaneously analyze information from disparate data sources spanning product and geographic lines, as well as external data sources. This capability not only increases businesses’ fraud detection, but also requires less time and fewer resources to identify potential risks.
Because bust-out or third-party application fraud often spans multiple product lines, individual portfolio-level fraud solutions may detect only small pieces of the puzzle. With its federated approach to simultaneously accessing multiple data sources, FICO® Identity Resolution Engine can put these pieces together and quickly reveal a comprehensive picture of fraud and criminal networks.

**Match**

One of the most challenging aspects of linking entities — determining who is really who — requires matching entity attributes pulled from data sources that are similar, but not exact. Most organizations’ data is fraught with inaccuracies and duplicates, as well as criminals’ falsified personal attribute information, resulting in entity resolution that produces too many false readings.

Identity Resolution Engine greatly narrows that margin with patented matching technology that accurately identifies connections between dissimilar data. Using more than 50 matching algorithms, Identity Resolution can detect slight variations in names, addresses, telephone numbers, SSNs, etc. Additionally, to avoid false positives, it can account for data anomalies such as misuse of data fields, visual scan errors and transposed data.

**Link**

In addition to properly identifying entities, Identity Resolution Engine quickly enables investigators to identify connections between entities, uncovering fraud networks. This capability is particularly beneficial in uncovering bust-out fraudsters operating across various portfolios, as well as insider fraud.

**Analyze**

Once entities and suspicious networks are indicated, Identity Resolution Engine applies additional analytics to score and prioritize matches. The score represents the risk level of each network and each individual within the network. The score can be impacted by several factors, such as an individual’s relationship with known fraudsters, suspicious relationships with bank insiders, or unusually large and diverse networks.

**Act**

Immediately following its analysis and identification of suspicious entities or networks — such as in application processing, or other reactive modes — Identity Resolution Engine sends real-time alerts to investigators. In addition, it supports investigative efforts with an intuitive link visualization interface. With graphical icons and associated and shared attribute information, visualization makes it easy for investigators to immediately review attributes of a person and his/her connections to other persons.
A flexible solution

FICO® Identity Resolution Engine is a critical component of a comprehensive application fraud management solution. This includes FICO® Application Fraud Manager, which offers sophisticated analytics to detect potential fraud; flexible business rules management to manage defined actions based on corporate parameters; case management capabilities to support workflow; and professional services to tie it all together. Additionally, Identity Resolution Engine is available as a standalone solution or can integrate with your existing fraud detection technology.

Additional benefits from FICO® Identity Resolution Engine:

Avoid privacy issues. The FICO solution does not require data from various sources to be kept in a central repository, avoiding the possibility of combining sensitive data or distributing it unintentionally or through a cyber attack.

The forensic value of data is not jeopardized. Many data-matching systems discard valuable forensic data as part of the data cleansing process. Identity Resolution Engine retains all of the originally entered information, eliminating rework if the case gets turned over to litigation.

Uncover most bust-out fraud rings and individual perpetrators with FICO Identity Resolution Engine.

Find out more at www.fico.com/ire