Pro Insight - Manual Review Solution

What is Pro Insight and what is included?
Ekata Pro Insight is the only global identity review solution that provides six ways to search, robust analytics and admin tools, direct workflow integrations, and a clear and focused user experience. Pro Insight enables organizations to assess identity risk, approve good transactions, and investigate fraud on a global scale.

What are the different ways to search and view identity data in Pro Insight?
Identity Review (the flagship search) is powered by machine learning and our Identity Network, and provides a comprehensive view of the identity behind a transaction by cross verifying digital and traditional data attributes. Identity Review results include a Confidence Score, insights into the score, and detailed information about each data attribute.

Pro Insight also offers deep dives which can be accessed from the Identity Review panel or by individual searches for: email address, phone number, physical address, person’s name, or business name. Deep dives provide additional information and in-depth details such as family members, household members, associated people, historical information, alternate phone numbers, and more.

What is the best way to access Identity Review?
Identity Review is best accessed through Deep Links which allow you to complete a full 5-in-1 Identity Review query directly out of your platform with a single click. Click here for more information about deep links.

How do you interpret Identity Review results?
Identity Review cross-verifies digital and traditional identity data attributes to return:

- Confidence Score
- Key positive and negative signals impacting the score
- Match statuses between email, phone, addresses, name, and IP
- In-depth details for each data attribute
- Network Insights
- Distance calculation map

The Confidence Score and reason codes are placed at the top of the screen and should be thought of as a comprehensive first look at the transaction as a whole. If the Confidence Score is high, this is a strong indication that it is a risky transaction. If the Confidence Score is low, this indicates that it is a lower risk transaction. The top positive and negative signals are placed beside the score to explain why the transaction inputs received that score.
Below the Confidence Score you can find the details of each data attribute. Warnings are highlighted in orange and indicate that there is either a mismatch or an invalid input. If you need to dive deeper into a particular attribute, you can click the “View more details” link located in the appropriate attribute column.

Network Insights are located in the panel below the results columns. They provide an additional layer of predictive analysis to determine fraudulent activity. Each of the Network Insight attributes are trained by our model to determine risk level. The three bar indicator next to each attribute is our evaluation of risk associated with that particular attribute. And finally, the distance calculation map is an interactive tool that shows a visual representation of the distances between the following inputs: phone, billing address, shipping address, and IP.

What are the positive and negative signals surrounding Confidence Score and how do they work?

Positive and negative signals are telling you the story behind the score. They are listed in order of importance, with the most influential signals at the top of the list. The symbol beside the signal indicates the strength of that signal on a scale of 1-5. These signals are dynamic and evolve based on the most current fraud trends seen by our Identity Network.

What are network insights?

The proprietary network insights are powered by the Ekata Identity Network which is derived from historical transactions and feedback data from our global risk conglomerate of thousands of customers. We surface these as three types of insights:

- **Popularity** indicates the number of merchants where an attribute (phone, billing address and/or shipping address) is seen in recent transactions.
  - Example - this phone number has been seen by X number of different merchants in last 90 days.
  - Fraud patterns it addresses - once a fraudster steals an identity, they may try to commit fraud at multiple merchants at the same time before the identity is flagged.

- **Velocity** indicates the number of times an identity attribute was seen in recent transactions.
  - Example - this phone number has been seen in X transactions over the last 90 days.
  - Fraud patterns it addresses - once a fraudster steals an identity, they may try to commit fraud through multiple transactions at the same time before the identity is flagged.

- **Volatility** indicates the number of times an attribute of an identity has changed over the last 90 days.
  - Example - X phone numbers have been associated with this shipping address in the last 90 days.
  - Fraud patterns it addresses - once a fraudster steals an identity, they may use different combinations of identity attributes to commit fraud.
What are signal strengths next to Network Attributes in Pro Insight?

Different threat levels have been determined using advanced machine learning techniques. These are relayed to the Pro Insight user through icon featuring 3 bars with one bar indicating a slightly elevated chance of risk, and 3 bars indicating a very high chance of risk.

What do the icons mean?

- No indications
- Low risk
- Medium risk
- High risk