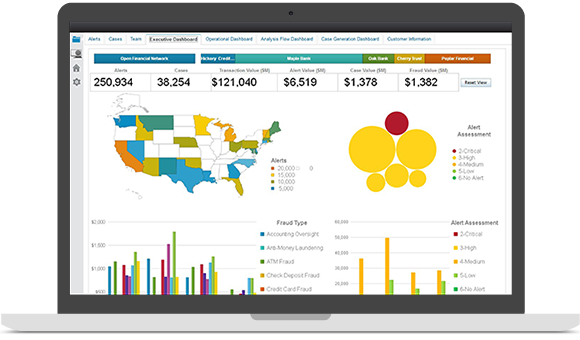
**Fraud Analytics Phases**

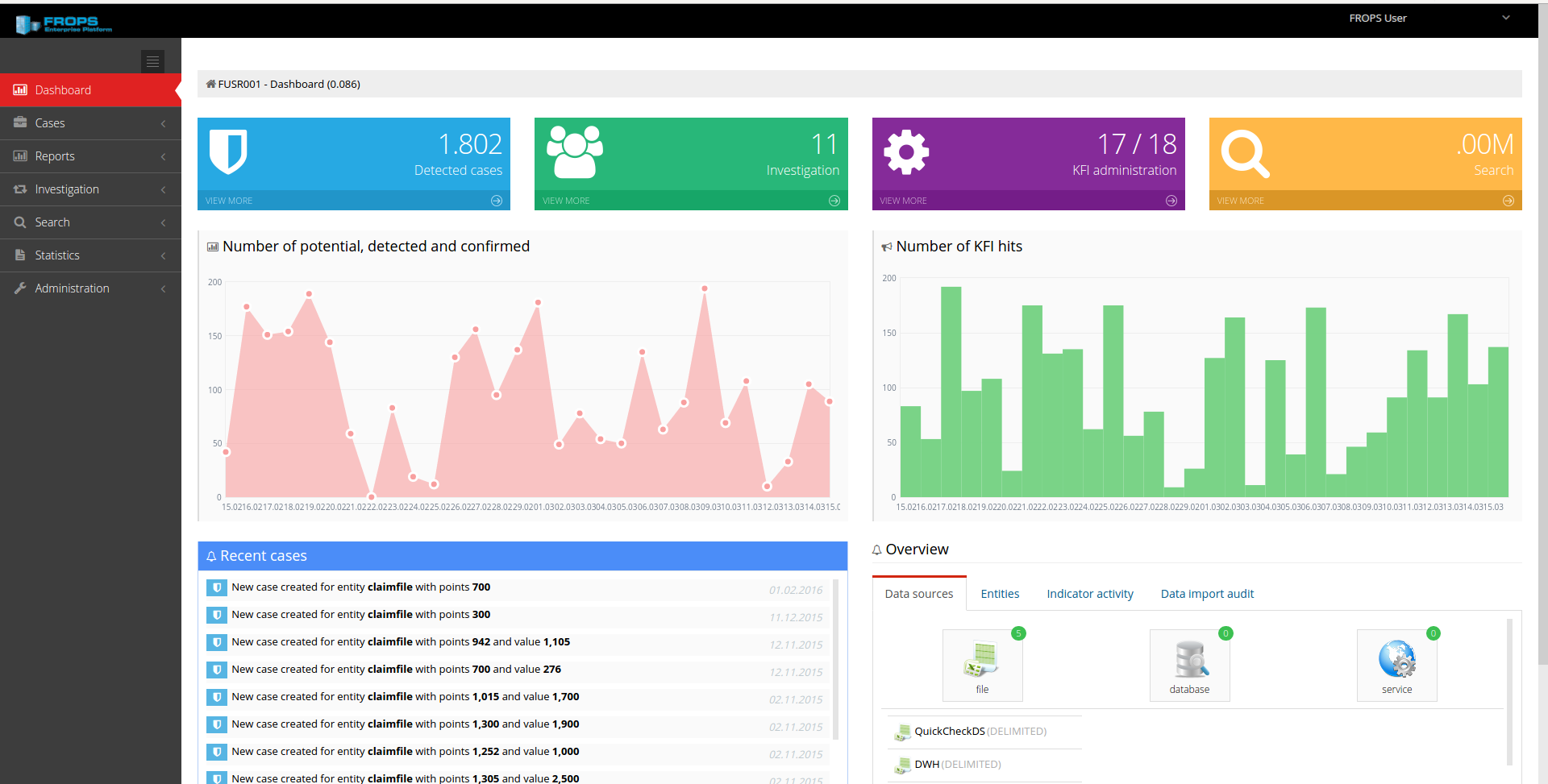
Fraud system lets organizations harness this machine data to meet a wide range of anti-fraud, theft and abuse team needs including:

* **Fraud detection** : real-time correlation searches or anomaly detection can identify and alert on fraud as it happens so organizations can act to prevent the fraud before it adversely impacts the bottom line
* **Fraud investigations** : quickly search and pivot through massive amounts of current or historical machine data to research possible fraud and to understand the "who, what, where, when and how" around a possibly fraudulent action
* **Fraud analytics and reporting** : make it easy to analyze, measure and manage fraud risk for a wide range of internal users
* **Enhance existing anti-fraud tools** : index event data from siloed tools to create an aggregate fraud score for a single transaction
* Create consolidated reports and dashboards to view enterprise-wide fraud risk on a single pane of glass

**Some examples for Fraud Dashboard UI design**



**a)**

**b)**

Following are some suggestions for fraud dashboards,

* Can categorize the fraud types and shows it visually like in the above example
* Can visually show the unusual patterns using real time data
* Can use alerts events to update the dashboard in real time
* Can use predictive models adapt to your customers and their individual behaviour patterns
* Can prioritize the details as in the above dashboard
* Give summarized numbers with separate boxes : to get a clear idea at the first sight
* Can use different pages with a left navigation bar Ex: above dashboard

**References**

* <https://feedzai.com/machine-intelligence/features/>
* <https://www.splunk.com/en_us/solutions/solution-areas/security-and-fraud/fraud.html>
* <http://ucustomersupport.com/11-uber-fraud-detection/>
* https://arxiv.org/pdf/1510.07165.pdf