BUILDING PROFILES

Fair Isaac offers the Merchant Profiles option to its Falcon Fraud Manager. It claims that this option can add up to 50% more detections of merchant fraud. When implemented, the Merchant Profiles option provides a score for each merchant to combine with the normal modeling score from Falcon Fraud Manager. This is a good example of how you can combine model predictions and profiles to create a more powerful fraud detection system, as depicted in Figure 17.1. Similar profiles can be built for customers in a commercial or credit context.

Many models can be built following this example. Each model could predict fraud under slightly different conditions. For example, the target variable in the KDD Cup 1999 data set included 24 categories of fraud. For the sake of illustration, the occurrence of fraud in any form was modeled in the earlier example. We could have restricted the model to just one of the 24 categories of fraud. Each of the models could be used to generate a fraud score for each type of fraud. These scores, plus the rules of thumb, demographic and firmographic data, and information from other external sources can be composed into a profile. From your score data, you could build multiple profiles that pertain to different types of fraud and different conditions of fraud (male, female, age, etc.). Potential predictor variables for a fraud detection model may come from data elements listed in the earlier section on how fraud detector systems are built. In addition to those variables, many time-based variables can be derived, similar to the ones used for the KDD Cup Network Intrusion model. The time spent on deriving novel variables is the most effective way to increase fraud detection rates.

If you are working on a fraud detection project in which the fraudsters can be identified, appropriate profiles can be built for various customer segments and combined with model scores to boost the detection rate. The combination of model scores and profiles constitutes the primary elements of a powerful fraud detection system.

DEPLOYMENT OF FRAUD PROFILES

These profiles can be loaded into real-time systems, and credit card applicants (for example) can be matched relatively quickly to known fraud profiles. Model scores and elements of profiles can be composed into business rules and programmed into SQL or some other production system interface. For example, some business rules resulting from this composition in a credit card environment might include

1. If the ZIP code on the application is not in the known list of the phone number area code → Fraud (a “red-flag” fraud indicator)
2. If the fraud model score is > 0.60 and the customer demographic profile matches that of a group of known fraudsters at the 85% level → Fraud

These business rules can be generated directly from rule induction engines, indirectly from decision tree algorithms, or inferred from combinations of neural net predictor variables with relatively high importance values.