Profiles of the past behavior and actions of both the fraudsters and the nonfraudsters must be built and employed in the modeling methodology.

Fraud can occur in many aspects of business:

- **Credit card fraud**: Stealing or counterfeiting credit card numbers, or nonpayment of accounts.
- **Charge-back fraud**: Transaction reversals after an item is shipped.
- **Check fraud**: Taking advantage of the “float” in time between writing the check and payment by the bank. In one form, the fraudster writes a check he knows is bad to delay payment until the check clears (“kiting”) or withdraws money from an account fed by a bad check and then abandons the account.
- **Application fraud**: Untrue statements on a credit application, leading to assignment of an artificially low credit risk.
- **Merchant fraud**: Involves the collusion of a merchant with another fraudster. One scheme is “white plastic fraud,” in which a merchant sends fraudulent sales drafts to a bank and pockets the sales draft payment by the bank.
- **Claim fraud**: Submitting inflated or false claims.
- **Life insurance**: False or “engineered” death claims.
- **Health care fraud**: False billings by health care providers.
- **Automobile**: Includes “soft” fraud of filing multiple claims and “hard” fraud of engineering accidents.
- **Property**: Includes arson and destruction of unsold property.

**HOW DO YOU MODEL FRAUD?**

There are three general approaches to modeling fraudulent events depicted in Figure 17.1.

Early fraud models employed expert systems to detect fraudulent events. An expert system is a collection of expert opinions on a number of decision criteria. Instead of sifting out mathematical patterns in a data set, these systems induced rules from the responses of a group of experts in the field. These rules can be coordinated into a flow chart leading to a decision. The problem with expert systems is that they are based on subjective inputs that may be contradictory. Subsequent fraud detection systems used automated rule induction engines, based decision tree technology, and fuzzy logic. Some of these fraud detection systems are still marketed today (iPrevent by Brighterion).

The most comprehensive fraud detection systems were developed by HNC Systems in the late 1990s (now owned by Fair Isaac & Co.). The Fair Isaac fraud detection systems Falcon Fraud Manager, eFalcon, and LiquidCredit Fraud Solution are built around a sophisticated system of predictive variables derived from extensive historical customer data. These predictors have been selected by many years of modeling fraud in many companies. The variables are submitted to a powerful backpropagation neural net developed by HNC Systems.