

National wireless telecommunications provider increases fraud identification in reduced time from shared data



Client

A leading nationwide provider of wireless telecommunications serves a high volume of customers in the majority of metropolitan areas. To answer the demands of existing — and potential — customers for increasing mobility as well as faster personal and business data communication, the provider is continuing to grow and diversify its coverage, products, services and wireless capabilities.

Challenge/Objective

Wireless phones are becoming increasingly common as a primary tool for criminals intending to commit a variety of subsequent fraudulent activities that cross a number of industries. For the wireless industry specifically, it's projected that annual losses of approximately \$275 million will result from subscription fraud alone. These losses, combined with other criminal activity associated with unauthorized network usage — in addition to the high cost of customer acquisition — made it critical for the provider to substantially enhance its fraud prevention strategy in a manner that was predictive and easily implemented.

A key goal was to determine a method for more aggressive detection of fraud during the new subscriber application process. This required the client to expand its existing fraud detection resources to encompass a faster, more effective method for identifying potentially fraudulent applicant data. At the same time, the client recognized the need to guard both consumers and the company against identity theft.

Overall, the client's objective consisted of continuing to meet the needs of its growing wireless network and maintain responsive customer service while significantly accelerating its fraud prevention activities, primarily during the processing of applications for new service.

Solution

To achieve its goal of faster, more effective prevention of fraud at the application stage, the company initiated a highly structured evaluation of all available fraud detection tools. As a result of this evaluation process, the company identified the significant benefits of the National Fraud DatabaseSM which — through the sharing of company fraud records — would enable reciprocal access to cross-industry fraud reporting through a "known fraud" database.

By contributing its own fraud information to the National Fraud Database, the company would realize the benefits of reviewing applications in tandem with real-time alerts of confirmed fraud as reported by multiple industries, including online retail, bankcards, credit cards and automotive lenders. This shared fraud database would thus speed application review and meet company objectives for identifying fraudulent applications while, at the same time, speeding the approval process for honest consumers and maintaining high levels of customer service.

Results

The client initially utilized the database in a proof-of-concept approach, using the National Fraud Database as a source for manually discovering and confirming fraud in newly activated wireless accounts to justify a business case for national rollout. After spending nearly a year in this initial phase and using approximately 27 percent of the available data, the client had confirmed fraud in 77 percent of the postactivation subscribers who had been highlighted by the data in the National Fraud Database. At the same time, cycle time for identifying the fraudulent subscribers had been reduced by 66 percent. The company was able to reduce losses per handset as well — by approximately 55 percent.

With positive proof-of-concept results, the client moved toward automated methodology, successfully using National Fraud Database in the preactivation stage on a trial basis in five markets.

The client has since implemented use of the National Fraud Database nationwide for all new accounts and sustained significantly positive reductions in application fraud, cycle time and handset losses. In addition to more effectively identifying fraud as well as doing so in a more timely and efficient manner, the company also is able to continue providing responsive customer service. Moreover, use of the database is helping protect consumers from the effects of identity theft; the company now can notify the intended victim prior to further use of — and damages resulting from — the stolen identity.

Statistical analysis on shared fraud data in the telecommunications, credit card and online retail industries proves that identity thieves do indeed cross industry lines when committing their crimes and that there are detectable patterns of fraudulent behavior. Accordingly, all of the industries participating in the sharing of fraud data are realizing significant, measurable benefits in terms of reducing fraud and related losses from using the National Fraud Database.