InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

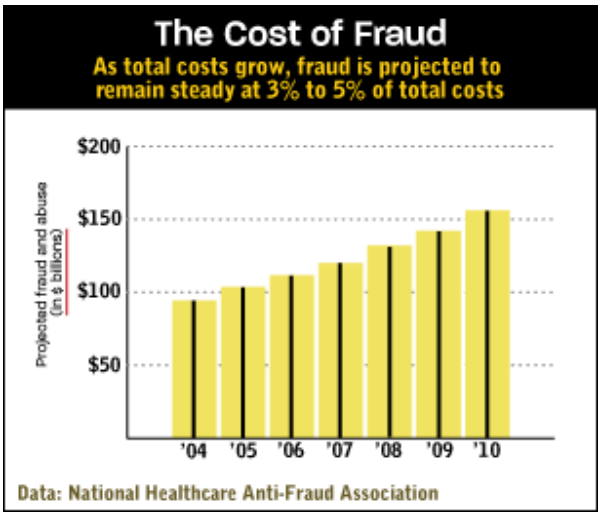
Filter Out The Frauds

Health insurers fight back against fake claims with fraud-detection software

By Charles Babcock and Marianne Kolbasuk McGee, InformationWeek
June 28, 2004
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=22101961

About a year and half ago, a Medicare examiner noticed a run on powered wheelchairs around Dallas. Health-insurance payouts for the chairs had soared by 300% in the region, and a quick review showed supersized payouts in parts of California and Florida as well. By the time the inspectors combed through all national data for wheelchair payouts, Medicare found that paid claims had tripled across 21 states in four years--a big anomaly.

The perpetrators got taxpayer-ID numbers and other data, submitted false claims for the $5,000 wheelchairs, and absconded from the country with millions of dollars, after evading investigators for four years, says Kimberly Brandt, a top fraud investigator for Medicare and Medicaid. Slow analysis was partly to blame. "We had seen a lot of little blips," she says. "But we couldn't pull all the data together."



Last September, Medicare slapped new software checks on its claims-processing system that identified powered-wheelchair claims and tested them for possible abuse--before a claim was paid. That's unusual in the health-insurance industry, which is projected to pay out $1.8 trillion across 4 billion claims this year. In the huge consumer-credit-card market, sophisticated software looks for cheats before companies part with their money. But most public and private health insurers examine only a small number of claims after the fact, hemmed in by industry pressure to pay claims quickly and a lack of technological tools. By looking at claims before they're paid, Medicare has been able to stop payment on $140 million in suspect wheelchair claims. "We'd like to move more of our fraud-prevention effort into a proactive mode," Brandt says.

That wish may soon become reality for broader categories than motorized wheelchairs. Armed with new software tools, two insurers--Aetna Corp. and Vista Health Plan Inc.--are applying fraud-detection techniques, historically used in the credit- card market, to examining all claims before they're paid. Fair Isaac Corp., a maker of statistical credit-scoring software for credit-card companies, retailers, and insurance firms that reviews 65% of worldwide credit-card transactions for fraud, this month released a new version for the health-care industry of its Payment Optimizer software, which applies fraud-detection techniques used by companies such as Visa U.S.A. and MasterCard International Inc. to health-insurance claims. Vista, which insures more than 350,000 people in Florida, is testing Fair Isaac's system to review every claim before it's paid. Insurers use their

claims-review systems--after payment--to look at only a fraction of the total, though that share can vary dramatically, from 5% to as much as half. "It's Fair Isaac's job to stay ahead of the criminal," says Bill Rushton, internal audit and fraud-prevention director.

Meanwhile, IBM is developing a software module for its Fraud and Abuse Management System, which is used by companies such as Horizon Blue Cross Blue Shield of New Jersey and Humana Inc. to review claims for possible insurance cheats. The module can review insurance claims for fraud before they're paid, and insurer Aetna plans to go live with it in October. When cheats are chased after they have their money, insurers are lucky to collect half of fraud losses. Instead, Aetna plans to unleash IBM's technology on up to 1 million daily claims that wend their way through Aetna's system, says business systems manager Ben Wright. "We think we will reduce the total loss," he says.

The software companies--and the insurers testing their latest technology--hope using prepayment analysis can reduce fraud levels to something closer to what they are in the credit-card industry: 0.06% of all transactions. Getting money back after it's been paid is more difficult--months of investigation typically lead to negotiated settlements or court dates that recover only 10 cents on the dollar. Sometimes, suspects simply walk away because enough evidence to indict can't be found.

Examining claims before they're paid "is the Holy Grail of the health-care industry," says Bill Mahon, who consults for insurance payers on fraud and is former president of the National Health Care Anti-Fraud Association, a nonprofit organization for sharing fraud information among insurance companies. Until recently, the industry took the point of view that examining claims before they were paid resulted in too little fraud detection and unacceptable delays. So for all its heavy-duty claims-processing systems and data-mining techniques, the health-care industry remains reactive to cases of fraud rather than trying to prevent them in the first place. Bilking Medicare, Medicaid, and private health-care plans "is a national epidemic," says Dave Hennings, 2004 chairman of the National Health Care Anti-Fraud Association. "We've been combating fraud from a reactive mode," he says. "IBM and Fair Isaac are moving to a more proactive mode, as in the credit-card industry."

The escalating costs of fraud may lead companies to look for new solutions. Estimates of the amount of U.S. health-care fraud range from 3% to 5% of filed claims. That translates into an estimated $57 billion to $94 billion in losses this year--equivalent to the annual tax revenue of the state of California at the high end of that range. And the problem is growing, at a 7% to 10% annual clip, according to Tim Delaney, chief of the Federal Bureau of Investigation's health-care fraud unit. By 2010, $154 billion in claims a year could be bogus. The problem is so persistent that some observers ask why the health-care industry can't do what the credit-card industry did over the last 12 years: cut fraud in half, or even greater, by using fraud-detection computer systems up front. Fair Isaac's version 2 software, released earlier this month, uses pattern-matching technology the company picked up when it bought HNC Software in 2002. The software can sift through claims and segment them by groups, such as the claims coming from out-of-network health-care providers preforming surgery. Traditionally, insurers hunt for fraud with rules-based data-mining systems, searching for claims that meet well-defined conditions, such as doctors who bill for 25 hours of office visits in a single day, and applying rules that can detect fraud. But if crooks vary their schemes from case to case, that method isn't as effective. Using pattern matching, insurers won't need to know all the details of how a scam operates before detecting it, says Fair Isaac health-care VP Joel Portice. Banks, insurance companies, and retailers have used HNC's technology to detect patterns from masses of complex data. "It makes sense to apply the same technology to health care," Portice says.

Sounds great, but there are lots of reasons it hasn't been done. Pattern-recognition systems such as Fair Isaac's Payment Optimizer or rules-based systems such as IBM's Fraud and Abuse Management can only see shades of gray in a mass of health-care claims. They seldom can put their digital fingers precisely down on fraud. That kind of intuition takes human investigators, who can decide whether the claims constitute fraud or abuse of the health-care system. Flagging more cases might mean delaying payment to legitimate providers. "We want to pay claims in a timely manner," says Rich Appel, Cigna Corp.'s director of special investigations. "It's a fine

line to walk when you work with these kinds of tools."

Another risk: gumming up the works that get health providers and patients paid on time. Prepayment analysis of claims threatens to create delays that run afoul of states' "prompt payment" laws, which require insurers to get their payments to doctors and hospitals in 14 to 45 days. The leaves little time to investigate suspicious claims. Forty-nine states have such laws on the books.

Payment delays rile clinics and doctors, whose offices depend on the cash flow, adds Steven Skwara, associate general counsel and director of fraud investigation at Blue Cross Blue Shield of Massachusetts. "Nowadays, the fraudulent claim looks exactly like the legitimate claim next to it," he says. When inspectors find a suspicious claim, they often ask providers for medical records, bills, and other documentation. "Thirty to 45 days can drop down the drain right there," he says. "Strictly electronic processing takes human eyes away from claims. The technology gain cuts both ways."

It's hard to tell the fraudulent claims from legitimate ones, says Steven Skwara, associate general counsel and director of fraud investigation at Blue Cross Blue Shield of Massachusetts.

Photo by Mark Ostow

Then there's the fact that computer programs--no matter how sophisticated--just aren't as good as human eyes at spotting fraud. With 4 billion health-care transactions to process a year and unyielding pressure to keep costs down, insurers' claims-processing systems "operate on a trust factor" that claims are valid, says Hennings at the National Health Care Anti-Fraud Association. The 1996 Health Insurance Portability and Accountability Act, a federal law passed to ensure the privacy of patients' medical records, was meant to reduce human involvement in claims processing, he says. But turning over that work to machines could cause some fraud to go undetected.

Even if pattern-matching systems work as advertised, they're not the whole answer. Vista Health Plan's Rushton says the company will combine Fair Isaac's new technology with software that sifts through claims after they're paid, looking for anomalies and evidence of known schemes as well as emerging scams sought by Fair Isaac. The post-payment data-mining technology can react to rules drawn up to detect known scams, such as bills for tests unrelated to a procedure or a provider that bills for the same patient twice. At Cigna, investigators this year have flagged 25 cases as "most suspicious" and needing further investigation, culling them from a larger pool of claims the software identified as unusual for some reason, says director Appel. He adds that selectivity shows the rules engine software is picking out only the most-worthwhile cases to pursue. Cigna is considering augmenting IBM's rules-based system with pattern-recognition technologies, such as Fair Isaac's. That could spot patterns hidden in the data that don't make sense. "Technology is just a piece of the puzzle," Appel says. "The investigators do the legwork."

That conservative approach to technology is typical of many insurers. Harvard Pilgrim Health Care Inc., a Boston-area health insurer, uses Fair Isaac's Payment Optimizer but so far utilizes it only to examine claims data after payment. The pattern-matching system is good at looking for "aberrations" in claims by comparing a provider to a peer group. If a pediatrician starts billing for allergy treatments, Fair Isaac may single out the claim as departing from the norm and thus suspect. Out of a group, "Fair Isaac picks out what's different," says Kimberly Grose, VP of network services operations. For now, Harvard Pilgrim is satisfied with using the system in post-payment analysis, she says.

Everyone in law enforcement and the insurance industry knows a new technology tool isn't going to solve the whole problem. Says the FBI's Delaney, "There's no easy fix." Aetna manager Wright adds that once fraudulent claims are detected, con artists will likely "just find another way to submit the claims. The game changes," he says. "Whether we can reduce the number of perpetrators, I'm not sure. But we think we will reduce the total loss."