Posted on Sunday, August 21st, 2011 [Text as submitted]

An e-ripoff of the U.S.

Disbursing public funds electronically sets up the federal government to be victimized by massive fraud.

BY MALCOLM SPARROW

Last week, a Los Angeles jury convicted a local pastor and his wife of fraudulently claiming $14.2 million from Medicare. The culprits recruited parishioners to help run fake durable medical equipment companies, and spent the proceeds on expensive cars and other luxuries. Assistant AG Lanny Breuer described their efforts as "persistent and brazen," and says "they treated the Medicare program like a personal till."

Around the country, a never-ending stream of Medicare and Medicaid rip-off stories suggest many people now use these programs as personal tills. In July 2010, authorities exposed and shut down a more organized scheme, charging 94 conspirators from five cities, who had stolen $251 million from Medicare.

Three months later, in October 2010, 52 members of an Armenian-American organized crime ring were arrested and charged with $163 million in fraudulent billing.

Scores of reports over the last decade catalogue completely implausible Medicare and Medicaid claims paid, apparently without a hiccup, for patients who were already dead, imprisoned, or previously deported from the country and forbidden to return. A significant number of claims involved *prescribing* physicians who were long-since dead.

What makes these health care programs so vulnerable to fake billings and at such a scale? It's not so much the healthcare policy itself, nor the program design; the vulnerability stems from the *payment mechanism* the government has chosen to use. Most Medicare and Medicaid funds are paid out electronically and automatically, in response to electronic claims received from a vast spectrum of providers. Most claims are adjudicated by computers using rule-based systems, with no human intervention at all. Fraud perpetrators have only to learn the rules; then they can submit thousands of claims electronically and with relative impunity. If they get things wrong, they'll receive helpful computer-generated messages explaining their mistake. Fraudsters are free to fabricate claims, or entire medical episodes, because the government's systems check for billing *correctness*, but not for *truthfulness*. The simple rule for get-rich-quick attackers, is "bill your lies correctly."

In 1995, as electronic claims processing was becoming more widespread, one seasoned Medicaid fraud investigator warned: "Thieves get to steal megabucks at the speed of light, and we get to chase after them in a horse and buggy. No rational businessman would ever invent a system like this." Nevertheless government continues to find the use of such systems attractive, mostly because the processing efficiencies are obvious and tangible.

This problem is not restricted to health care. Federal and state agencies increasingly disburse funds through such *Electronic Signal In, Electronic Payment Out* (ESI-EPO for short) systems. The economic stimulus package, for example, included 56 different tax provisions projected to cost $288 billion. Ten of these have already been designated high-risk, with the fraud threats centered on tax-credits administered through the ESI-EPO method. Submit a qualifying tax return electronically and, if it has been completed correctly, out will come an electronic payment with no human intervention and little or no validation of the supporting evidence.

Payments for the stimulus fund's first-time homebuyer credit were found to have included $9 million paid out to 1,300 prisoners, 241 of whom were serving life sentences when they purportedly bought homes. More than 10,000 taxpayers received credits for homes also claimed by other taxpayers, and one home was claimed by 67 separate claimants. The homebuyer program paid out more than $23 billion in total, and claims sampled after the fact showed dead people and young children showing up as "home buyers," in patterns eerily reminiscent of healthcare fraud.

Another stimulus component, residential energy credits, disbursed $5.8 billion in 2009 for residential energy-saving improvements. Once again, "homeowners" included prisoners and infants, and—based on a review of a random sample of claims—30% of the recipients appeared not even to own their own homes.

The Earned Income Tax Credit program, which has a much longer history, is projected to cost $64 billion annually in 2010 and 2011. The last available estimates put the improper claims rate between 23.9% and 28.7%. It was the EITC program, with its "easy money fast" features, (unusually fast, thanks to the advent of electronic filing and Refund Anticipation Loans) that originally attracted many crooks to the tax domain in the early 1990's. Use of the tax system to disburse a broader array of payments (as tax *credits*) has since provided these crooks a rich menu of targets.

The recipe for disaster is now clear. Whatever the nature of the payments—welfare supports, reimbursements, health claims, tax credits, incentive payments or subsidies—pay them electronically. Set up the system with honest claimants in mind. Allow claims, and any supporting documentation, to be submitted electronically. Set the administrative budget low enough that the bulk of the claims have to be paid on trust, without verification. Use computerized rule-based systems to ensure consistency and predictability in the way claims are paid.

In terms of the underlying public policy objectives, this is exactly the right thing to do, serving the genuinely deserving in a most efficient manner. Unfortunately, this also creates perfect targets for fraud: giant, predictable, utterly transparent electronic cash machines, with insufficient audit and investigative resources behind them to cope with the inevitable onslaught.

To make things really dangerous, add a degree of urgency to the public purpose (as with the stimulus package). Urgency tends to trump caution, and raises policymakers' perception of the "business-acceptable risk." And if it's a really *valuable* program, supporters and officials will be loath to hear any criticism of it, which will incline them to discount or downplay any reports of extensive fraud.

It is no longer sensible to disburse public funds, on trust, through electronic systems. The commensurate risks are enormous, and seriously underestimated. Organized crime groups, prisoners, and a host of other criminal entrepreneurs troll government websites looking for programs with these vulnerabilities. Such systems must now either be fortified with substantial resources for routine validation or, preferably, be phased out altogether through structural reforms.

Fixing these vulnerabilities offers substantial promise for long term deficit reduction, in a form that both political parties could support. But one important political obstacle remains: finding the courage to admit how serious and pervasive this problem has become.

Absent some fundamental reassessment of electronic payment systems, we are doomed to continue dealing with serious fraud threats on a case-by-case rather than on a structural basis. Happily, each case detected provides some (false) assurance because it was, after all, *detected*. And each successive scandal offers an opportunity for officials to proclaim, once again, their "zero-tolerance" for fraud in vital public programs.

I have zero tolerance for fruit flies. But they just keep coming, despite my protestations, until I put the fruit away.

Professor Malcolm K. Sparrow of Harvard's Kennedy School of Government is the author of "License to Steal: How Fraud Bleeds America's Health Care System." He is also deputy chair of the Recovery Independent Advisory Panel, appointed by President Obama to advise on protecting the integrity of the economic stimulus package.