

## **2011 Fraud Trends**

Even as overall fraud rates plateau, CUs could be more often targeted—and low credit risk members will need special consideration and protection.

By Thomas Oscherwitz

*January 2011*

Fraud strategies at credit unions have assumed increasing importance due to an evolving fraud landscape and new economic conditions.

### **CUs More Often Targeted?**

On the surface, identity-related fraud appears to have stabilized in recent years. The number of fraudulent incidents reported by consumers to the Federal Trade Commission's [Consumer Sentinel Network](#) actually dropped from 314,000 in 2008 to 278,000 in 2009. ID Analytics' own experience with leading credit providers across multiple industries is that fraud rates have reached a plateau.

ID Analytics' clients reported a spike in first-party fraud at the outset of the recession, but have seen a recent drop-off in this crime. In first-party fraud, an individual will manipulate his own identity slightly (e.g., changing or adding the middle initial to their name, slightly modifying a home address, or Social Security number) in the hope of getting credit to which he otherwise would not be entitled. With the economy improving, these illicit credit-seeking strategies have diminished.

In addition, between 2007 and 2009, identity fraud linked to credit cards declined from 23 percent to 17 percent, fraud related to electronic fund transfers dropped from 7 percent to 4 percent, and fraud associated with wireless and landline telephones dropped from 14 percent to 6.6 percent of the cases reported by consumers to the FTC. These drops are not surprising as megabanks and national wireless carriers have bulked up their anti-fraud programs and fraud detection technology.

However if the big banks are doing a better job of driving away fraudsters, the fraud shops of credit unions and smaller banks may well see more pressure. It is the nature of fraud and fraudsters to migrate to areas of least resistance. Credit unions should expect increased attacks as fraudsters respond to tougher screening at larger institutions.

### **Serving Key Members**

After several years of retrenchment, financial institutions across the board are aggressively trying to acquire customers. Credit card issuers, including credit unions, were expected to mail out approximately 2.5 billion card offers in 2010,

up from 1.39 billion in 2009, according to [Synovate](#). This new round of solicitations is different from previous markets in that creditors are targeting a narrow band of low risk consumers with good credit.

This tightly focused credit environment will continue to be with us for a while. In its October 2010 [Senior Loan Officer Opinion Survey on Bank Lending Practice](#), the Federal Reserve asked senior bank loan officers when credit standards might be loosened and return to their long run norms. A substantial portion said that those standards wouldn't ease before 2012.

To win over this cadre of low risk consumers and to protect their own key members, credit unions are seeking to minimize consumer friction in their verification processes. When checking for fraud, there's always the possibility that a member will become annoyed and feel that the credit union is putting up barriers for them getting service. In good economic times with high member growth, lenders can tolerate the loss of a certain number of good members, but in current economic conditions really good members are much harder to find. Credit unions can't afford to lose members by making sign-on for electronic banking services too onerous or by rejecting legitimate customers because of an inaccurate classification of their identity risk. In 2011, credit unions will continue rebalancing their management of fraud and credit risk. Expect those who work in your fraud shop to get a few more calls this year.

*Thomas Oscherwitz is VP/ government affairs and chief privacy officer at [ID Analytics, Inc.](#), a leader in consumer risk management. He is also a former U.S. Senate legislative expert on ID fraud.*