MSA Identity Monitoring Services
(including examples)

One of the most powerful upgrades to CLC's Identity Theft Services is to provide **"Identity Protection AND Monitoring"** of a member's Social Security Number. This service endeavors to prevent non-credit oriented ID thefts. The benefit is known at **"MSA ID Alert**." It is made available to **My Secure Advantage™ (MSA)** and **MSA ID Protect** members.

ID Monitoring provides a national name and SSN (Social Security Number) /DOB (Date of Birth) search. This member service screens a vast number of national databases, including credit bureaus and major data aggregators, for any use of a member's SSN and name **(including name variations - e.g. John Smith and Johnny Smyth),** as well as data mining of the member's address and DOB. These national database searches can provide **early and critical indicators that there is usage and/or fraudulent activity taking place.** ID Monitoring works to catch activity that often **precedes** fraudulent credit and debt creation, as well as identity fraud that would never hit a credit bureau-- such as an identity thief using a member's SSN/DOB to take a job or buy a car (with cash) in another city or state.

Whether a member opts for this service or not, if the member becomes a victim of Identity Theft, **MSA** provides a Name/SSN search as a part of **MSA** Identity Theft Fraud Resolution Services. These Identity Theft types will seldom, if ever, appear on the victim's credit report. **MSA ID Alert** is one of the few ways that a potential victim can identify many of the more dangerous types of Identity Theft (which are not "credit" related), such as:

- Criminal arrests and issuance of arrest warrants in other jurisdictions
- Criminal convictions in the victim's state or in another state
- A job taken in another city or state, using the victim's name and/or SSN
- DMV registrations for licenses (or cash motor vehicle transactions) in another city or state
- Real property sales or leases in another city or state, where a public database is used

MSA ID Alert also provides: (Members **must opt-in** for coverage)

- An Identity Fraud/Identity Theft risk score to the member
- Identified fraud/identity theft discovered (during any monthly scan) will initiate the **MSA** managed fraud recovery process
- Assistance in reading and understanding **MSA ID Alert** findings/results and Identity Scoring.

MSA ID Alert can also help to identify **"Synthetic"** Identity Theft. This occurs when the thief is utilizing the victim's SSN, but is using a different name, address or date of birth. It is now the fastest growing form of identity theft.

MSA ID Alert often gives notice of the thief's activity very early in the fraud process and aids in pinpointing the location of the thief and criminal activity. This is one of the primary reasons the **MSA ID Alert** process assists in establishing the location, arrest, and prosecution of approximately (1) in (12) identity theft thieves.

EXAMPLES OF CASES COVERED BY MSA ID ALERT**

****Many types of fraud are <u>not detected</u> by traditional credit monitoring services. These cases are estimated to be as high as 80% of identity theft cases, which take place in today's data-drenched markets.**

Medical ID Theft

1. An individual's purse is stolen with the health care card/identity (driver's license). The thief later checks into a hospital ER room to give birth. The thief uses a false address for check-in and billing purposes. The health insurance company later refuses payment due to a change in blood type, claiming the actual insured/victim did not have a baby. The debt is then assigned to a collection firm and the victim is found on a skip-trace by the collection firm. Collection efforts and lawsuits then begin against the victim for the significant uninsured cost of the ER room and birth.

2. A woman's new health card was stolen from her mailbox. When she never received it, the company sent her a replacement card. Several weeks later, the Sheriff, a deputy and a Hospital Social Worker showed up at her door with a warrant to search her house for drugs because two days earlier, a thief had checked into the hospital using her health card and information and delivered a drug dependent baby. The thief and baby checked out of the hospital, but Social Work Services was notified. The victim was a 68-year-old woman.

Social Security Number Theft

1. An individual illegally purchases another person's SSN and applies for work in another state. The thief then obtains employment using the victim's SSN and begins filing tax returns by either under withholding taxes due, or by receiving income tax refunds. The victim, upon filing tax returns in the usual course, is billed by the IRS for under reporting income (or is told that the refund has already been issued to the thief.) The victim's tax records are now completely distorted and the IRS is seeking back taxes, interest and penalties against the victim through levies and garnishments.

2. A family files their taxes claiming their young daughter as a dependent and is subsequently audited by the IRS because their daughter has already been claimed as a dependent on a thief's return in another state.

Department of Motor Vehicles

1. An individual has purchased or stolen the name and SSN of another person. The thief purchases a motor vehicle/motorcycle for cash and proceeds to register the vehicle in another state under the SSN of the victim. The vehicle is later involved in a wrongful death and a lawsuit for significant damages is filed against the victim as the registered owner.

2. A thief shows a modified copy of the victim's driver's license to the police at the scene of an accident. The thief is charged for the accident and does not appear for his court date. A bench warrant is issued for the arrest of the victim. Also, the victim's car insurance rates are increased because of the accident.

Criminal Convictions and Outstanding Arrest Warrants

An individual has stolen the identity of another person and is committing crimes in another state. The thief has both a criminal record and has an outstanding arrest warrant for failing to appear in court on a current matter. The victim is involved in a traffic accident/ticket and the police data scanner shows the victim has an outstanding arrest warrant. The victim is immediately arrested and taken to jail, leaving the family members behind at the scene.

Real Property Transactions

An individual has purchased or stolen the name and SSN of another person. A quitclaim deed or cash transaction occurs using the SSN for tax assessment purposes. The property is later foreclosed upon due to delinquent property taxes. The victim's credit ratings/scores are destroyed after the foreclosure is reported to the (3) Credit Reporting Agencies.

Payday Loans

On line "Payday Loans" generally do not require identity verification. All that is needed is a bank account into which the "borrowed" money can be paid. The thief fraudulently opens a bank account (in the victim's name) and may share a stolen pay-stub with either the bank or the lender. The "loan" is withdrawn later and the victim finds out about the debt when a collection call or letter arrives. No credit report was needed, so no credit monitoring report/alert ever takes place.

Instant Credit Cards Issued On-Line (small sums of $300-$400)

Like payday loan, some credit card companies issue cards with very little proof of identity required, all of which may be stolen. Since the sum borrowed is so minimal, no credit report is requested and the card is issued. The thief uses the card, fails to pay the debt and a collection call or letter is the first that the victim hears about the debt now past due.

"Synthetic Identity Theft"

In any of the above examples, a theft becomes "synthetic" when a name, DOB or SSN, or combinations thereof, are used in part (not together) in different locations or states. This is the fastest growing form of ID theft, as various pieces of a victim's identity become more and more available on the Internet, and on the blogs, where criminal trading of stolen identity takes place for very short periods of time in order to avoid detection and criminal prosecution. An early warning that parts of the victim's identity may be in motion can buy time to quickly act and prevent serious damages to the victim's credit score and credit profile.