

Interview with an Identity Theft Detective

By Patrick Ritchie

To get a true feel for identity theft you need to talk to someone who deals with it everyday. I interviewed a detective who spent four years investigating identity theft related crimes. Talk about an interesting conversation!

Almost 100% of the time these ID crimes are connected to drugs, most commonly methamphetamines. When the police bust a meth lab it is not uncommon to discover a room filled with boxes of mail. People on meth tend to not sleep for days and this gives them plenty of time to steal mail and then go through it. Not to mention going through dumpsters looking for sensitive information.

Catching mail thieves will sometimes lead back to the meth lab for a larger scale bust. Since stealing mail is a Federal crime, law enforcement can leverage the scale of the crime to get more information out of the criminal. The mail thief is at the bottom of the totem pole when it comes to identity theft, but they are a good source of information leading to the arrest of the ring leader.

Identity thieves typically work in specialized areas. The guy who steals mail teams up with someone who knows how to make fake identification. From there they team up with someone who can make bogus checks. A name taken off of a bank account can then be made into an ID with the criminal's face. Making a check with the account numbers from the bank statement then allows the thief to go out and write checks against an existing account. It may take weeks before the victim catches on to what is happening. A lot of times the thieves will make purchases at a store and then go to a different location to return the merchandise for cash.

Typically ID thieves are opportunists who are repeat offenders. Some of them believe identity theft is a victimless crime because they think the bank incurs the loss, not the consumer. They look for the easiest way to steal a buck. One ID thief told the detective, "I am better off taking an ID for \$30,000 than robbing a bank for \$5,000 and facing an automatic 10 years." It can be hard to identify these people because the crime may not be discovered for a stretch of time. A store camera may recycle every couple weeks. By the time the crime is discovered the tapes could have been erased. Some stores have digital cameras that can record months of footage. The best thing to do is report these crimes as soon as they are discovered to have a better chance of identifying the culprit.

Identifying the suspects even when there is a photo can be challenging. If it is not someone the detectives are familiar with, they only have a face, no name or any other way to find the person. A lot of times the photo will be forwarded to other agencies and jurisdictions to see if it is someone they recognize. Ultimately the photo may end up in the jail with the hopes that the suspect will be picked up on other charges at some point and the jailers will recognize the suspect.

Once a suspect is caught, the entire ring may soon come crashing down. The guy writing the checks may turn in the person making the checks. In return, the check maker rats out the person who provided the names.

In some cases the fraud did not stem from mail theft, but from database theft. This leads to other possible criminal charges because now there may be a business that had its client information compromised. The original suspect may lead back to a computer tech that took client information from a business. This is not uncommon, especially when the detectives interview victims and find a common thread.

Imagine this scenario: You visit a medical office once. You provide your name, your date of birth and your social security number so the visit can be paid for by your insurance company. A year later you receive a letter stating that your personal information may have been compromised. Apparently, many recent victims of identity fraud in the area have a common link. They had all visited this particular medical office. How did your information and the information of fellow patients get into the hands of ID thieves? The computer tech for the business was stealing the information off the company computers and selling the information in exchange for drugs.

Scary stuff. And it happens more often than we'd like to think.

Patrick Ritchie is the author of "The Credit Road Map," a practical guide to navigating the world of credit. The book can be purchased at www.TheCreditRoadMap.com or on www.Amazon.com.

Copyright © 2006 Success Road Map Press, reprinted with permission.