

# THE OUCR NEWSLETTER

**APRIL 2007**

## **Rocky Start, huh?**

Okay. Admittedly this second newsletter is a bit late in coming. Our intent is to produce a newsletter every month, or every other month. However, just like the rest of you, we've been busy. We'll try to do better in the future!

## **What's new?**

After years of telling you that we were "planning" on a revision of the O-NIBRS program, it has actually begun to happen! We are happy to announce that we have signed a contract with **SMART Public Safety Software, Inc.** to rewrite our antiquated and extremely user-*un*friendly O-NIBRS Repository! This revision of the Repository brings with it a truck load of benefits, not just for OUCR staff, but for contributing law enforcement agencies and all users of OUCR data.

For OUCR staff, it means extremely rapid processing of records. At present, it can take a day or more to process data from a single large agency. The new system will process an equal amount of data in minutes. We'll have better access to the data that you provide us. The current O-NIBRS system is a "black hole" that sucks in data, but gives very little back. Better access to the data means that we can more efficiently fulfill our mission of providing statistical information to the vast number of end-users who request special research and reports. We will also be able to utilize the latest technology in hardware/software which provides better accuracy and more stability to the system. Anyone remember DOS? Well, that's what our current O-NIBRS system runs under. You're right, that's so eighties!

For law enforcement agencies this revision of O-NIBRS allows for on-line reporting. This is especially beneficial to smaller agencies that want to participate in O-NIBRS, but can't afford the expense of a computerized report management system (RMS). The new O-NIBRS repository will allow agencies to report directly into the database without the need for a separate RMS. In essence, OUCR will become their RMS. Larger agencies that already have an established RMS will have the benefit of either reporting directly into the O-NIBRS repository or submitting an extract from their own RMS as they do now. Law Enforcement will also have direct access to their records in the O-NIBRS system. This eliminates the need for an agency to call OUCR to run the records and the time delay to mail or fax the information back to the agency.

Perhaps the greatest benefit to law enforcement with the revision of the O-NIBRS repository is the creation of an investigative database exclusive to law enforcement. We have added more than 50 data elements to this revision. Combined with the 100+ data elements the current O-NIBRS system already collects, this database promises to provide a substantial amount of information for investigators. Some of the information available (to law enforcement for investigative purposes only) includes names, person status (victim, offender, suspect, arrestee, witness, etc.), addresses, identification numbers, telephone numbers, vehicle information, and a

lot more. Those agencies that already have computerized RMS's know the benefit of being able to make an inquiry on a name or address and get a list of offenses that may be associated. Agencies that are on a network where all local jurisdictions share computerized information also know the benefit of sharing that information. What the new investigative database will do is provide sharing of data between agencies that are not already connected to a shared database. For example, Pendleton PD could discover that a subject they are investigating is also a suspect in a burglary in Newport. Opposite sides of the State, but able to share data.

Taking Oregon's investigative database a step further, the new O-NIBRS repository will be Oregon's gateway to the FBI's new National Data Exchange (N-DEx), which takes data sharing to the national level. The FBI has already awarded a contract with a software developer and work on N-DEx is currently underway. With the new O-NIBRS repository expected to become operational on roughly the same timeline as N-DEx, we expect to participate in "Phase 1" of the implementation of this national program toward summer's end.

Oregon's investigative database and N-DEx will fill many of the "gaps" that are found in LEDS and NCIC files. They are not meant to replace LEDS and NCIC files, but to complement them.

Finally, this revision provides a searchable database for the public which includes non-law enforcement agencies, other governmental agencies, the news media, educators and students and the rest of the almost innumerable host of people who routinely seek information from OUCR. The "public side" of the O-NIBRS database will obviously not provide personal information on any person, street addresses, telephone numbers, or any other sensitive information. However, it will provide the opportunity for anyone to make inquiries such as how many burglaries were reported for a specific time period in a given area, city, zip code or county. These searches will also produce crime maps showing general locations where crimes have occurred. Law enforcement inquiries will produce more detailed crime maps giving specific locations and other information regarding individual offenses.

Agencies that already report in the O-NIBRS format don't have to worry that they'll have to abandon their expensive report management systems and buy something new. Even though we are adding another 50+ data elements to the system, agencies that already report O-NIBRS data may continue to report using their same software. We have already contacted most of the software vendors who have provided O-NIBRS RMS's to Oregon agencies regarding the upcoming changes to the O-NIBRS system. Generally, the response has been that upgrades to current systems will be relatively simple. None have expressed any anxiety over the forthcoming changes. Even if agencies do not upgrade their RMS's to the newer O-NIBRS format, they will continue to be able to report in the format we're currently using.

## **Before you ask...**

As mentioned above, O-NIBRS collects a lot of data. Some of that data is quite sensitive, such as the name of a victim. The public needs to be assured that **no sensitive data** of any kind is **ever** made available to anyone who does not have a legally defined, mission critical need. This means that **only** law enforcement agencies performing an on-going criminal investigation will be allowed to view information that may be deemed sensitive. If that sounds familiar, it should. LEDS and NCIC rules also stipulate looking at sensitive records such as criminal histories, warrants and DMV records must be for on-going, mission critical purposes. Even though those records are "public records", accessing them through LEDS or NCIC is forbidden except for official purposes. You've all heard the stories of the dispatcher who "ran" her new boyfriend or the officer who "ran" a potential babysitter and suffered the consequences for doing so. Some have lost their jobs because of abusing the LEDS/NCIC system. The same will apply to

sensitive data collected in O-NIBRS. Access to sensitive data in the O-NIBRS database will be protected by 128-bit encrypted passwords and logins that will never be made available to the public. Since access to sensitive data is only available by logging into the system, when an inquiry is made, we'll know. Make sure your staff is aware of that.

Even though only law enforcement agencies will be able to view full records reported to OUCR, we understand that there may be some agencies that do not wish to share their data with others. We're not exactly sure why they wouldn't want to, however. Agencies on regional computer systems already know the many benefits of sharing information between agencies. In this day of stretched budgets and under-staffed police departments, law enforcement agencies need every tool available to them. Sharing information is an invaluable tool.

Still, if a law enforcement agency insists that their data not be shared in either the Oregon investigative database or N-DEx (or both) that is their option. In other words, **just because an agency submits their data to OUCR, it doesn't mean they are surrendering control over it. Each law enforcement agency contributing to O-NIBRS will be able to determine if sensitive information is to be shared with other law enforcement agencies.** We hope that each agency will see the benefit of sharing information, but ultimately it is the individual agencies' decision.

More on the O-NIBRS repository replacement as things develop...

## **Topic of the Month – Identity Theft**

There are few questions that we get anxious over more than questions about identity theft. That's because determining if identity theft has occurred can be so complicated with a rat's nest of victims, offenses, locations, jurisdictions and property.

### **Hurdle #1 – Definitions**

Oregon has 2 Revised Statutes (ORS) pertaining to identity theft and impersonation. ORS 165.800 specifically defines the crime of identity theft as follows:

***“Identity Theft.*** *A person commits the crime of identity theft if the person, with the intent to deceive or defraud, obtains, possesses, transfers, creates, utters or converts to the person's own use the personal identification of another.”*

ORS 165.800 defines *another person* as being a “*real or imaginary*” person. You are real, Fred Flintstone is imaginary. The ORS defines a person's *identity* as any of the following: *a person's name, address, telephone number, driving privileges, Social Security number or tax identification number, citizenship or alien identification number, employment status, employer or place of employment, employee number, maiden name of a person's mother, financial account numbers (e.g. credit card, debit card, checking account, etc.), signature, e-mail name, e-mail signature, e-mail address or account, a person's photograph, a person's date of birth (combined with other identification!) or any other personal identification number.*

Obviously, some common sense needs to be used when investigating identity theft. If I mistakenly write down your phone number instead of mine on a check or form, I'm not stealing your identity. It is a mistake. The intent of the offender must be taken into account.

Before we move on, let's take a look at ORS 162.365, which deals with the crime of criminal impersonation.

***“Criminal Impersonation*** *A person commits the crime of criminal impersonation if with intent to obtain a benefit or to injure, deceive or defraud another the person falsely impersonates a public servant and does an act in such assumed character.”*

The key words to remember in this ORS are *“impersonates a public servant”*. The ORS goes on to say that the *“public servant”* being impersonated need not be a real person or from a real government agency. So, if Officer Jones from the Oregon State Highway Patrol pulls you over and wants you to get out of your car, you may want to do so in a well lit and heavily populated area. Oregon has no “Highway Patrol”, we have State Police who are troopers, not “officers”. “Officer Jones” is most likely an imposter who is up to no good.

So far we've looked at the 2 ORS's that deal with people claiming to be someone or something that they are not. The final definition we need to address is from the FBI.

***“(Fraud) Impersonation*** *Falsely representing one's identity or position, and acting in the character or position thus unlawfully assumed, to deceive others and thereby gain a profit or advantage, enjoy some right or privilege, or subject another person or entity to an expense, charge or liability which would have otherwise been incurred.”*

The definition presented by the FBI essentially combines the 2 statutes mentioned above. The actor is assuming a person's identity or office (real or imaginary) for personal gain of some kind.

### Hurdle #2 – ORS vs. OUCR vs. O-NIBRS

Remember, it is sometimes difficult, confusing or outright impossible to directly relate an Oregon Revised Statute with a UCR definition. Depending on the totality of the circumstances, an offense may fit more than one UCR definition. With identity theft we'll further compound the problem by providing 2 reporting formats; OUCR and O-NIBRS. With the revision of the O-NIBRS repository, we will have a specific identity theft code that O-NIBRS agencies will be able to use, but that's still 6 months (+/-) away. For today, in April of 2007, we have to make identity theft “fit” somehow into our 2 existing reporting formats. In the older OUCR format, the best one can do is report an identity theft offense as **“Fraud – By Deception”**. We get a bit closer in O-NIBRS (the current version) by reporting the offense as **“Fraud – Impersonation”**.

### Hurdle #3 – Is it Identity Theft, Forgery or Both?

There *is* a difference, you know. Simply put, identity theft is when the offender in some way assumes the identity of another. Forgery is uttering a representation as the real thing, or altering something to make it appear to be something else. If a person obtains another's credit card number and uses it to run up a huge bill making on-line purchases, we're looking at identity theft. The person is using a real credit card number and has assumed the identity of the victim. If the offender then signs the victim's name on an order form, that's forgery, as well. However, if the victim writes a check to the offender and then the offender alters the check to a higher value, that's forgery only. The offender has not assumed the victim's identity, just altered the check.

## Hurdle #4 – How/What to Report?

Here is a scenario to help us wade through this identity theft problem. To those of you who sat through our presentation at the 2006 LEDS Workshop, this will be a repeat, sorry.

**Scenario:** On August 13<sup>th</sup> the offender rummages through the victim's trash and finds pre-authorized credit card applications. The offender completes one of the applications and receives a credit card in the victim's name (John Dough). The offender then uses the credit card to make purchases at 4 local businesses on September 4<sup>th</sup>, 5<sup>th</sup> and 2 on the 7<sup>th</sup>. Several weeks later the victim is contacted by the credit card company about not paying anything toward the \$12,000 on the now limited-out credit card.

What offenses do we have to report? First of all, there is the theft of the credit card application. Yes, it is a stretch, but for argument's sake, let's assume that the victim could remember the day he threw the application in the trash (that is NOT at the curb yet!) and has a pretty good idea of when it was taken. Then there are 4 offenses each of credit card fraud, identity theft and forgery.

For OUCR agencies, here's a summary of how these offense would be reported:

- August 13<sup>th</sup> – 1 incident of larceny-other for the theft of the mail from the trash.
- September 4<sup>th</sup> – 1 incident with the offenses of fraud-credit card, fraud-by deception and forgery-other.
- September 5<sup>th</sup> – 1 incident with the offenses of fraud-credit card, fraud-by deception and forgery-other.
- September 7<sup>th</sup> – 2 incidents, each with the offenses of fraud-credit card, fraud-by deception and forgery-other.

The offenses of fraud-credit card should be obvious. The offender used a credit card that didn't belong to him to obtain a benefit he wasn't due. The offenses of fraud-by deception are the identity theft. During each incident the offender assumed the identity of the victim to cause the retailer to believe the offender was actually the victim. The offenses of forgery-other are for each of the times the offender signed (forged) the victim's name on the sales receipt.

For O-NIBRS agencies, your records would look something like this:

### August 13<sup>th</sup>

- Offense Segment with offense of larceny-other.
- Victim Segment for John Dough as victim of larceny-other.
- Property Segment for mail documents.
- Offender Segment for the bad guy.
- Individual Segment for John Dough.
- Individual Segment for the bad guy.

### September 4<sup>th</sup>

- Offense Segment with offenses of fraud-credit card, fraud-impersonation, and forgery-other.
- Victim Segment for business as victim of fraud-credit card.
- Victim Segment for John Dough as victim of fraud-impersonation and forgery-other.
- Property Segment for the property obtained by using the credit card.
- Offender Segment for the bad guy.
- Individual Segment for John Dough.
- Individual Segment for the bad guy.
- Individual Segment for the complainant (cashier, store manager, etc.)

### September 5<sup>th</sup> & 7<sup>th</sup>

- 3 more incident records similar to the record for September 4<sup>th</sup>. 1 each for the 3 remaining incidents.

As you can see, in O-NIBRS the code used for identity theft has changed from fraud-by deception to fraud-impersonation. Also, please note that the original victim, John Dough, is carried through each of the incidents. In each incident he is the victim of identity theft and forgery.

Once the O-NIBRS repository is replaced, agencies reporting in O-NIBRS format will replace fraud-impersonation with fraud-identity theft. Of course, that will happen after O-NIBRS agencies have the identity theft code added to their software by their software provider(s). Until that time, O-NIBRS agencies should continue to report identity theft as shown above.

For those agencies that may be looking at the amount of information required by O-NIBRS for each incident for the first time, do not be intimidated by it! All of this data is information you already collect on your incident reports. Your incident report has the victim, doesn't it? Offender (suspect) information? Property information? Complainant? If you have a computerized report management system that produces a monthly extract for OUCR, you are excluding a large amount of data. O-NIBRS asks that your submission contain more of the data that you already have in your system. O-NIBRS is software-driven. It cannot be done on paper, so don't even worry about being asked to do it that way!

## **We Get Questions...**

*Q: If we report identity theft using the new O-NIBRS identity theft code (when it becomes available), how does it go to the FBI if they don't have an identity theft code themselves?*

A: The O-NIBRS repository converts all O-NIBRS codes into the correct FBI codes before we submit it to the FBI. That will include the code for identity theft. You report "identity theft" to us and we will submit "impersonation" to the FBI.

*Q: One of our officers contacted a subject on the street late one night. The subject was intoxicated and had no identification with him. He identified himself as "Daffy Duck". Is that identity theft?*

A: We'd like to see how this person "acted in the character or position" of Mr. Duck! No, this is not identity theft. Was the officer deceived by this person? Did the officer believe this person really was Daffy Duck? Did the officer really believe this intoxicated subject had the mental culpability to commit the crime of identity theft? Or, was he a drunk trying to be funny?

*Q: How about if the person uses a lesser known cartoon character name like Race Bannon? What about a character from a TV show, a movie or a book?*

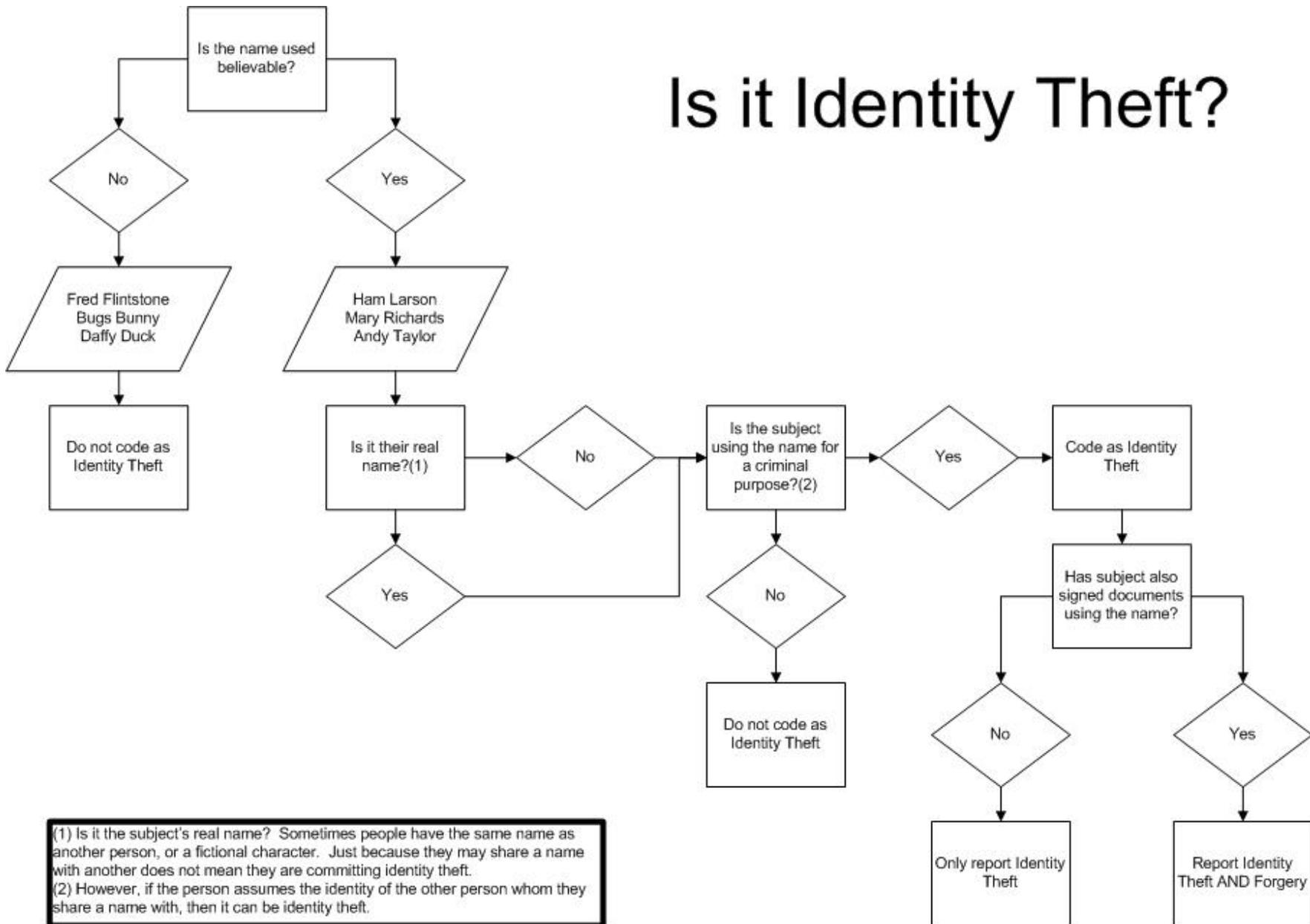
A: In theory this could actually work as an identity theft. As long as the offender isn't trying to convince people he is *the* Race Bannon from the Johnny Quest Cartoons. If the offender is just using the name to fit a created identity to defraud or make some kind of gain unlawfully, that fits both the ORS and the FBI definition. You have to admit that "Race Bannon" is a more convincing name for a person than "Daffy Duck". Now, if he starts talking about how he's the personal body guard of a child genius who on a weekly basis saves the world from evil scientists and monsters from space, he's probably a walk-away from some facility rather than a criminal using an assumed identity.

The second and third questions point out a very important consideration about identity theft... and crime reporting in general: the use of common sense. If a subject told you that he was Daffy Duck, Mickey Mouse, or the Green Hornet, would you REALLY believe him? Do you REALLY think he expects you to believe him? Of course not. However, if he identified himself as Darin Stevens (1), Dan Tanna (2) or Tony Nelson (3), you might believe him since they could be real names of real people. You need to look at the totality of the circumstances. Is the name believable? How are they using the identity? What do they stand to gain? Are alcohol or drugs a factor? Is there a chance of a mental condition such as some kind of delusion where the person really thinks he is who he says he is?

Yes, a fictitious persona is allowable as identity theft, but Daffy Duck? C'mon...

(1) Husband in "Bewitched". (2) Private Investigator in "Vegas". (3) Astronaut in "I Dream of Jeanie".

# Is it Identity Theft?



(1) Is it the subject's real name? Sometimes people have the same name as another person, or a fictional character. Just because they may share a name with another does not mean they are committing identity theft.  
(2) However, if the person assumes the identity of the other person whom they share a name with, then it can be identity theft.