SAKI
SEXUAL ASSAULT KIT INITIATIVE
Reform. Accountability. Justice.

RTI INTERNATIONAL

# Cold Case Review and Investigation:
## What to Do If You Do Not Receive a CODIS Hit

## Overview

This is the third installment of the SAKI TTA Team's Combined DNA Index System (CODIS) follow-up brief series. This guidance document focuses on investigative steps to follow if forensic evidence from a sexual assault kit (SAK) uploaded into CODIS does not return a match or "hit." For additional information on CODIS and the SAK testing process, see the SAKI TTA brief, Sexual Assault Kit Testing Process.

You may not have a CODIS hit in all situations. One of three possible outcomes may occur when performing a search in CODIS:

- Match to a known offender (CODIS hit)
- Match to an unknown offender (CODIS hit)
- No match (no known profile in CODIS).

A sample cannot be uploaded into the system if you do not have enough of the suspect's DNA.

**If you have enough DNA for a sample, then that sample can be uploaded into CODIS to search for a match. Even if there isn't a hit, that profile will remain in CODIS as a potential match for future investigations.**

As investigators, your team will be left without a suspect when (a) an uploaded profile does not match to an existing offender or a forensic sample or (b) a large enough DNA sample does not exist for upload into CODIS. The first scenario provides an advantage because in the future, the profile can be searched in CODIS and may provide a match for a different crime. If the suspect commits a CODIS-eligible crime in the future, that individual's DNA profile may be collected and uploaded into CODIS; the CODIS upload creates an offender match. In the second scenario, your team needs to rely on other investigative methods to bring a potential suspect to justice.

The following sections provide an overview of alternative investigative techniques when you do not receive a hit in CODIS. These techniques should be generally followed for all CODIS hits. The SAKI TTA Team encourages you to move forward with cases regardless of the status of forensic evidence; this approach will help to avoid delays in bringing justice for victims.

## Review the entire case file, including existing evidence

- Check your evidence tracking system for other evidence associated with this case.
- Conduct a physical inspection of the evidence (if located) to determine if it has anything that can be tested (e.g., DNA or fingerprints).
  - The SAKI TTA Team recommends reviewing the available evidence with members of the crime laboratory and crime scene.
- Determine what else can be done with evidence gathered from the crime scene.
  - Was something missed?
  - Can anything else be tested? DNA processing has greatly advanced in the last several years.
- Provide the crime laboratory and crime scene teams with a background of the case and your evaluation about what evidence should or could be tested. Then ask the crime laboratory personnel and crime analyst for their input about the best evidence to test and the best testing methods.
  - Evidence that is located should be reviewed, ranked for potential probative sampling, and then tested.
    - Latent fingerprints are often overlooked in these situations. If available, have them reviewed for database entry.

## Review available data

- Examine phone data (e.g., call detail records [CDRs], historical Global Positioning System [GPS], texts) for multiple parties, including the victim, suspect, and witnesses.
  - Data may reveal a new lead, new areas that should be checked for video to establish a suspect, and/or information the victim did not mention.
    - Were there other potential witnesses?
  - Attempt to locate copies of CDRs, historical GPS, subscriber information, and text messages. Companies may store data for a long time.

- GPS/CDRs may reveal a new pattern of travel if a cell phone was taken during the incident.

- Review data associated with social media and cloud accounts for all parties (e.g., victim, potential suspects, witnesses).
  - Social media accounts have messages, posts, and GPS data (if enabled). Obtaining these data will most likely require a search warrant.
  - Companies oftentimes do not delete social media accounts immediately.
  - Cloud accounts may include accounts through a cell phone carrier, internet search companies, and cloud-based storage companies.
    - These accounts can show messages, files, and GPS. Cloud accounts may also show who the victim contacted (and vice versa) around the time of the event.
- Determine if a cell tower "dump" was completed and if the data were reviewed.
- Review the sexual assault nurse examiner/forensic medical personnel report.
  - Is there new information or something you missed previously?
  - What were the victim's injuries?
- Conduct both local and national sex offender registry checks.
  - Is there a pattern of attacks? If yes, was the suspect in your area when your incident occurred?

## Complete additional investigative work

- Figure out if there were witnesses near the attack.
- Determine potential suspects from the time of the event through crime analysis.
  - Were they ruled out entirely? If not, conduct an entire work-up and find out why.
  - Do you have a surreptitious DNA sample to compare to your suspect's sample (in the event of a CODIS entry with no known match)?
  - Do you have a search warrant for DNA based on what you learned during your review of the case (in the event of a CODIS entry with no known match)?
- Re-interview parties (e.g., victim, witnesses, detectives) and review past statements made by these parties.
  - Did the victim provide all the relevant details to detectives assigned to the original case? Was this a potential consensual partner?
  - Does the evidence support the victim's account of the incident?
    - If not, determine if there is another issue at hand (e.g., issue related to faithfulness, family/culture, or regret).
  - Consider interviewing the victim's family members to assist in establishing a potential suspect or motive that began this investigation.
    - Proceed cautiously as the victim's family may not be aware of the crime.

## Examine the crime scene

- Visit the crime scene (if possible) and see what, if anything, has changed. Photograph the area for future reference.
- Determine if witnesses live in the area (e.g., established businesses that have remained there since the incident).
- Conduct witness canvass in the area to see if anyone knows about the incident.
  - People located during these canvasses may have information the original investigator did not uncover.

## Research other crimes in the area around the time of the event

- Was there a crime trend (e.g., burglary, automobile theft)?
- Were there any crimes with suspects who had similar physical descriptions as the suspect in your incident?
- Were there minor sex crimes in the area that could be linked to the same suspect?
- Were there similar crimes that were not captured by your police department? Review news stories from the time frame of the incident.

## Contact other local law enforcement agencies to learn about similar cases

- If the event occurred near a transportation hub (e.g., bus depot, train yard), check with nearby companies about other possible incidents.
- Check nationally via the Federal Bureau of Investigation (FBI)'s Violent Criminal Apprehension Program (ViCAP), Law Enforcement Information Exchange (LInX), or other national search engine(s).
- Check private paid services (e.g., CLEAR, Accurint).

## Conduct research online

- Perform internet searches in hopes of revealing information to assist in your case.
- Review blogs, news reports, and victim and/or witness accounts that people posted.

## Encourage interagency cooperation

- Develop a team to review this case; this approach allows for a broader knowledge base and new ideas.
- Advise team members that all input is needed.
- Ask for support from your agency and other local agencies.
- Understand that collaboration takes time, but it lessens the need to meet and discuss the evidence several times (because you began the process as a group).
  - **Your agency:** Consult your agency's crime analyst. Ask the analyst to review the crime and check for patterns in the time frame the incident occurred. Also have the analyst check for potential matching patterns from around the time of the incident.
  - **Other agencies in your area:** Request assistance from analysts at other agencies. These agencies may have records on crimes that match or are similar to your agency's records.
- Request assistance from the FBI. Bring the file and discuss the case; the FBI: Quantico group[1] will assist in the investigation by building a profile of your offender.
  - The FBI's ViCAP can assist in locating patterns of criminal behavior across the country; ViCAP offers the following support:
    - Putting you in touch with the agencies
    - Partnering with your agency to develop a profile of your offender
    - Providing investigative assistance for your case.

## Ensure a successful investigation

- Be empathic.
- Employ active listening and trauma-informed interview practices with the victim and witnesses.
- Follow the evidence and science.
  - Ensure that what you are being told is, in fact, possible.
  - Were there evidentiary items that need to be reviewed (e.g., DNA, fingerprints)?
- Keep an open mind and explore every possible angle using your experience and that of other experts.
- Collaborate! You should not do this alone.
- Never give up.

Authors:

Lt. Jordan Satinsky, Montgomery County Police Department

Sgt. Jim Markey (Ret.), Phoenix Police Department

[1] This group brings together many disciplines to assist in your case.

This project was supported by Grant No. 2015-AK-BX-K021 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the U.S. Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice. **For more information, visit www.sakitta.org.**

SAKI 11703 0218