Directions for completing "security information" declaration

The problem

Under Minnesota law, data held by a government entity are presumed to be public. Minn. Stat. 13.03, subd. 1. The password provided to identity theft victims as part of the FBI's Identity Theft program is public data under this presumption.

The solution

The responsible authority for a government entity can declare certain data to be "security information" as that term is defined in 13.37. If applied in this case, this declaration will result in the password being classified as private data on individuals and therefore not accessible to the public.

The "responsible authority" is an employee who has the role within a particular government entity. By law, the county sheriff is the responsible authority for that office. For police departments, the responsible authority is the city employee is the city administrator or city clerk.

To implement the attached security information declaration, you will need to insert the name of your organization and the mane of the responsible authority. Once the responsible authority has signed the declaration, keep it in a safe place.

Also, once the security information declaration is signed, any documents containing the identity theft victim's password will need to have the password redacted or removed before the document is released. This redaction will be in addition to other redactions that are based on other provisions of law such as redacting the victim's Social Security number that is protected by Minn. Stat. 13.355.

Determination of Classification of Data at Jordan Police Department.

The Jordan Police Department is entering victim data in the Federal Bureau of investigation's (FBI's) Identity Theft File. One of the data elements entered into the Identity File is a password the victim can use to identify him/herself to law enforcement.

Under Minnesota law, data held by government are presumed to be accessible to the public. Minn. Stat. 13.03, subd.1. The purpose of the password is to help a victim of identity theft prove that they are not the perpetrator who stole the identity. This password will serve its intended purpose only if it is not accessible to the general public.

Minn. Stat. 13.37 permits the responsible authority for a government entity to designate certain data as "security information" if the disclosure of those data would "substantially jeopardize the security of information, possessions, individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury." If the victim's password is not protected by this determination, it will be accessible to the public and will further jeopardize the security of the victim.

Therefore, as the Jordan Police Department's responsible authority under the Minnesota Government Data Practices Act, Minnesota Statutes, Chapter13, I have determined that the password received by an identity theft victim part of using the FBI's Identity Theft File is "security information" as defined in Minn. Stat. 13.37, subd. 1 (a).

By: [JORDAN POLICE OFFICER COMPLETING FORM] Date

***THIS FORM TO BE SENT TO FORWARDING AGENCY IF APPLICABLE.

CONSENT TO CREATE A FBI IDENTITY THEFT FILE

By signing this document, I hereby give Jordan police Department permission to enter my personal data into the Federal; Bureau of Investigation's (FBI's) Identity Theft File. This information may include, but is not limited to, my physical description and other identifying information including my name, date of birth, social security number, the type of identity theft, photograph, fingerprints and a password created by me or a law enforcement officer for future verification of my identity by law enforcement.

I understand that this information is being submitted as part of a criminal investigation of a crime of which I was a victim. I am giving this information voluntarily so that it will be available to law enforcement entities that have access to the FBI's National Crime Information Center (NCIC) files for any investigative or law enforcement purposes authorized by the NCIC. I am providing this data in order to document my claim of identity theft and to obtain a unique password that I can use for future verification of my identity by law enforcement.

I understand that the FBI intends to remove this information from the NCIC active file five years from the date of entry. I also understand that I may submit a written request at any time to the Jordan Police Department to have this information removed from the active file before the five years are up. I further understand that removing this information from the active file will prevent it from being accessible to law enforcement and criminal investigation entities connected to the NCIC. However, it will remain in the FBI's data system as a record of the NCIC entry until its deletion is authorized by the National Archives and Records Administration.

The privacy Act of 1974 (5 U.S.C. 552 a) requires local, state, or federal agencies to inform individuals whether disclosure of that individual's social security number is mandatory or voluntary, the basis of authority for requesting the information, and the uses which will be made out of it. Disclosure of your social security number is voluntary; it is being request pursuant to 28 U. S.C. 534 for the purposes described above. The social security number will be used as an identification tool by the FBI system. Consequently, failure to provide the social security number may result in a reduced ability to make such identifications or provide future identity verifications.

_____ _____

SIGNATURE DATE

_____

PRINTED NAME

NOTICE ABOUT PROVIDING YOUR SOCIAL SECURITY NUMBER

The federal Privacy Act of 1974 (5 U.S.C. 552 A) requires local, state, and federal agencies to inform individuals whether sharing that individuals social security number is mandatory or voluntary, the basis of authority for requesting the information, and the uses which will be made of it.

Disclosure of your social security number is voluntary; it is being requested pursuant 28 U. S.C. 534 (Acquisition, Preservation, exchange of Identification Records and Information) for the purposes explained below.

The Jordan Police Department is asking you to provide us with private data, your Social Security number. This agency will forward that number to the Federal Bureau of Investigation (FBI) as part of the criminal investigation for the crime of identity theft, which you state had occurred. Your private information will be added to the FBI's National Crime Information Center (NCIC) Identity Theft File. You will create or help a law enforcement officer a unique password that will enable you to verify your identity with law enforcement.

You do not have to supply your Social Security number and may legally reuse to give it. The Social Security number will be used to identify you in the NCIC system. Consequently, failure to provide the Social Security number may reduce law enforcement's ability to verity your identity or to investigate the crime.

Your personal information, including your Social Security number, will be available to law enforcement and other agencies that investigate financial crimes and have access to the FBI's National Crime Information Center (NCIC) files. These agencies include police departments and sheriff offices in all states. Additionally, the FBI and other federal agencies will have access to your information for the purpose of investigating identity fraud and other violations.

Your Social Security number will also be available to the Minnesota Bureau of Criminal Apprehension and NCIC employees or contractors whose job duties require that they access the data. The Social Security number may be shared as required by court order or sent to the state auditor or the legislative auditor for auditing purposes. The FBI has auditing requirements and those responsible for that will have access to your private data.

By signing this notice, I affirm that I have read this notice and that I unde4rstand that I may refuse to give my Social Security number to this agency. I understand that this agency will submit my Social Security number, along with other personal information, to the FBI's National Crime Information Center Identity Theft File, where it will be able to be accessed and used by local, state and federal law enforcement agencies for the purpose of investigating identity theft and other crimes. I understand that I will leave with a unique password that I may use in the future to verify my identity.

_____ _____

SIGNATURE DATE

First Name:	Middle Name:	Last Name:
Address:	City:	State/Zip:
DOB:	Sex:	Race:
Height:	Weight:	Hair Color:
Eye Color:	Skin Tone:	Citizenship:
Place of Birth:	Ethnicity:	Scars/Marks/Tattoos:
Medical Conditions:	Type of Theft:	ICR:
Password:	Phone #:	Social Security:
OLN #:	OLN State:	MISC:

Fields that are **HIGHLIGHTED** are **REQUIRED** for entering Identity Theft Information into NCIC. This information **MUST** also be listed in your report. This page is only a reference to ensure all of the required information is gathered at the time of the call to supplement the details in your report regarding the identity theft.

If the victim does not have any scars/marks/tattoos, you **MUST** write N/A

Indicate if the identity theft is one of the following:

- Checking or Savings Account-Includes check fraud, unauthorized use of ATM, debit, or check card; and opening a fraudulent checking or saving account.
- Credit Card-included unauthorized use of or opening a fraudulent credit card account.
- Government Documents or benefits- Includes Driver's license issued or forged, social security card issued or forged, fraudulent tax returns, government benefits, and other government documents issued or forged.
- Internet or email-Includes opening new internet accounts (email, web site, etc.) or unauthorized use of existing accounts.
- Loans-Includes real estate, auto, auto lease, personal or business loans.
- Phones or utilities- Includes opening new accounts (wireless, pager, cable, etc.) or charges to existing accounts.
- Securities or other investments-includes opening or trading on existing securities or investment accounts.
- Other type-Includes all types of Identity Theft that do not fall into any other category.

The victim generated password shall be up to twenty (20) alphanumeric characters. The password will assist the victim in identifying themselves to Law Enforcement during potential police encounters. The password should be determined by the victim when possible.

The victim Social Security number is *not required* BUT STRONGLY ENCOURAGED. See attached Social Security number disclosure statement.