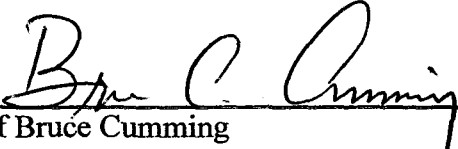


Santa Clara County Police Chiefs' Association
Identity Theft Protocol

SANTA CLARA COUNTY POLICE CHIEFS' ASSOCIATION



Chief Bruce Cumming
Chair, Police Chiefs' Association of Santa Clara County

6-30-09

Date

Santa Clara County Police Chiefs' Association

Identity Theft Protocol

Goal: To provide Santa Clara County Law Enforcement Agencies with a resource for accepting, investigating, and referring identity theft.

Practice: Agencies should thoroughly investigate all reported identity thefts, as well as theft-related crimes that generally accompany identity thefts. Officers should provide assistance to victims in contacting consumer protection agencies, work with them to acquire evidence from affected business entities, and cooperate with federal, state and local law enforcement agencies undertaking related and/or parallel investigations.

This protocol expresses the consensus of member agencies as to how ID Theft cases are to be investigated. The protocol permits individual police agencies to make modifications in order to meet their agency regulations.

I. GENERAL PROTOCOL

- Investigations of identity theft will be conducted as required by California Penal Code Section 530.6 which states that victims may file a report with their local law enforcement agency that has jurisdiction over his/her residence or place of business.
- Identity theft offenses most often involve the unlawful use of victims' personal identification to defraud merchants or financial institutions. Accordingly, identity theft investigations must necessarily extend to include related property thefts, burglaries, forgeries and other income producing crimes.
- The agency that has jurisdiction over the victim's residence shall take a report, provide the complainant with a copy, and begin an investigation.
- If the suspected crime was committed in a different jurisdiction, the local law enforcement agency shall forward a copy of the report to the law enforcement agency where the suspected crime was committed for further investigation.

Note, that California Penal Code section 786(b)(1) now provides that identity theft jurisdiction can also include the county in which the victim resided at the time the offense was committed.

- Referral to another agency should take place after full consideration of the jurisdictional authority now provided under Penal Code section 786(b)(1). The decision to refer to another law enforcement agency

should take into account the convenience of the victim, the location of witnesses and evidence, and the relative strength of the case in the victim's home jurisdiction versus the jurisdiction where the offense was committed. The originating agency should follow through with all aspects of an investigation up to conclusion of the court process, if the majority of the investigation resides within the jurisdiction of that agency, or if the victim lives in the jurisdiction of that agency and several separate ID theft offenses can be consolidated in one prosecution.

II. INITIAL REPORT PROCESS

- Agencies are mandated to take a report from a resident within their jurisdiction or the victim's place of business in their jurisdiction.
- Officers shall make all reasonable efforts to obtain suspect information, seize evidence and provide victims with resource information to assist them in dealing with banks, credit unions and other businesses to restore their identity.

See Attached: Identity Theft: Patrol Officer's Basic Guidelines

See Attached: Identity Theft Investigator's Checklist

See Attached: Know your Rights: California Identity Theft Victim Rights

- Officers should ask victims to begin gathering documentation (bank and credit card statements, letters from creditors, merchant account statements, etc.) and provide them to the assigned detective for follow-up. Note that, under California Penal Code section 530.8, merchants, financial institutions and other business entities must provide identity theft victims with copies of fraudulent documents that contain or otherwise present those victims' stolen personal identification. Identity theft victims have the option to direct that such documents be provided to the law enforcement agency responsible for investigating the offense. Information obtained through section 530.8 demand letters can significantly expedite criminal investigations. Accordingly, officers should work with victims to obtain evidence through that process in appropriate cases.

See Attached: Requesting Information on Fraudulent Accounts: A Guide for Identity Theft Victims

See Attached: Identity Theft Victim's Request for Fraudulent Transaction/Account Information

- Officers should advise victims to obtain credit reports from the three major credit bureaus, (Equifax, Experian, and Trans Union) and place "Fraud Watch" notifications on their credit reports. They should also be advised to destroy credit cards associated with compromised accounts (until new cards

are issued) and to contact the DMV in cases where drivers' licenses were lost, stolen, or misused.

- Officers should request the victim's fingerprints, a copy of their driver's license and take a photograph of the victim. Officers should explain to the victim that the purpose for taking the fingerprints is to prevent any further identity theft, as well as to provide accurate identifiers upon comparison of the victim's and suspect's fingerprints. If the officer lacks capability to take fingerprints in the field, the agency should ask the victim to provide fingerprints at an appropriate law government facility. This can be done in much the same way as agencies use for fingerprinting applicants in pre-employment checks.

III. INVESTIGATIONS

The following steps can be taken at the onset of the investigation:

Department of Justice: Obtain a photocopy of the victim's driver's license and thumbprint to comply with new Department of Justice Identity Theft database requirements.

Pending Court Hearings: If the victim has been falsely arrested and/or posted bail on a warrant issued in his or her name or signed a promise to appear, then they must appear in court, regardless of whether or not they are innocent of the original charge. Failure to do so could result in a new "Failure to Appear" (FTA) charge against them and a new warrant being issued.

In either case, as soon as possible investigators will have to either notify the D.A. on criminal matters or notify the Court on traffic matters that an impersonation has occurred.

Drivers License Actions: If an impersonation victim's license is in jeopardy due to an FTA or suspension due to an Admin Per Se or court order, investigators may take steps to take the license out of jeopardy while an investigation is conducted.

Wage Garnishments: If an impersonation victim's wages are facing garnishment or they have received a bill to pay a fine from the Department of Revenue (DOR) or Franchise Tax Board, investigators may contact the DOR in an attempt to resolve the issue.

Car Insurance: A victim's car insurance rate may be affected due to an impersonated ticket accident or arrest. Investigators may notify the traffic court or contact the DA as appropriate.

Employment Jeopardy: If a victim's employment or potential for employment is jeopardized by a false conviction record on his or her identity, investigators may notify the traffic court or contact the DA as appropriate.

IV. VICTIM RESPONSIBILITIES

- Victims should be advised to check their credit reports for unauthorized charges as well as to check for fraudulent credit applications under their name. Credit fraud victims may also be asked to complete an affidavit of fraud for the creditor. The Federal Trade Commission has developed a generic affidavit that can be downloaded from the FTC website. Victims may save time by checking with the creditor to see if they will accept the FTC affidavit. The website is located at www.ftc.gov. Victims may also contact the California Attorney General's Office at www.ag.ca.gov in order to obtain additional information about ID theft prevention and response.

See Attached: ID Theft Affidavit

See Attached: Instructions for Completing the ID Theft Affidavit

- Victims may also contact the California Department of Justice Identity Theft Registry at 888-880-0240 and the Federal Trade Commission 1-877-IDTHEFT.

V. AVAILABLE RESOURCES

- Coordinate or refer to the local task force REACT/ High Tech Crimes Task Force.
- Refer to Federal Agencies (FBI, Secret Service, and Postal Inspectors) as appropriate.
- Coordinate with DMV Investigations Unit for California driver's license.

VI. TRAINING

All agencies are encouraged to have a training plan for their members, including:

- Informational Brochure to assist victims with the steps needed to restore their identity.
- Peace Officer's Standards and Training (POST) Identity Theft Investigation training.
- Roll-call training for patrol officers detailing the elements of the crime(s), and the need to obtain detailed information from the victim concerning the type of account(s), as well as the name of the issuing bank or financial institution.
- Orientation training on the Identity Theft Victim database maintained by the Department of Justice (DOJ).

VII. PENAL CODE SECTIONS

((Refer to 530.5 (a), 530.6, 530.7, 530.8, 529 and 484 (e))

VIII. CONSUMER PROTECTION LAWS

Refer inquiries to:

District Attorney's Consumer Unit:
70 W. Hedding St., West Wing
San Jose, CA 95110
Email: Consumer Protection @da.sccgov.org
(408) 792-2880

IDENTITY THEFT PATROL OFFICER'S BASIC GUIDELINES

Taking the Victim Report

Who takes the initial report?

You do. According to PC 530.6(a), an ID theft victim may make a report to the law enforcement where he or she lives or works.

What should your report include?

Identify the victim and/or reporting party/parties.

Specify which identifying information was unlawfully used.

Secure a specific and unequivocal statement that use of the ID was not authorized.

Eliminate the possibility of ID use by family or friends who may have presumed authority to use the ID.

Determine how and where the identifying information was used (i.e., to commit a fraud or theft, to open a credit account, to obtain employment, to conceal identity, etc.)

Inquire if a point-of-compromise is known.

Collect the available evidence from the victim and book it into evidence.

Ask the victim to collect and retain all not-yet-available documents related to the incident (credit reports, bills, etc.) until contacted by follow-up investigators.

Ask the victim to complete a PC 530.8 request (see "Identity Theft Victim's Request for Fraudulent Transaction/Account Information")

Determine if there are additional victims and attempt to contact them as well.

Where should your report be referred?

In addition to the usual inter-departmental routing, you should also forward a copy of your report to the agency that has jurisdiction where the theft or unauthorized use occurred.

If a suspect is known, refer a copy of your report to the agency where the suspect resides.

Victim Assistance

See: Know your Rights: California Identity Theft Victim Rights

Witnesses Other than Victims

Collect statements and contact information from all witnesses to the unauthorized use (e.g., in a retail transaction, determine which specific employee or sales clerk had contact with the suspect).

In business cases, identify the custodian of records and note contact information.

Identify and secure evidence

Conduct identification procedures as per your agency's policy

Determine if surveillance tapes exist and request copy as appropriate.

If in a suspect-controlled location, check for notebooks, computers and digital storage media, access cards, checks, and other ID documents that may be relevant.

Suspect Present or Contacted

Confirm Identity

Determine suspect's actual identity, residence address, telephone/cell phone numbers, etc. Obtain CDL info.

Suspect Interview (Subject to usual Constitutional procedures)

Identify accomplices, co-conspirators, and instrumentalities used by the suspect.

Determine how the identity information was obtained, and whether there was any claimed authority or permission to use the information.

Determine whether/where the suspect used the identity information in other locations or businesses.

Follow-up Investigation

See: Identity Theft Investigator's Checklist

IDENTITY THEFT INVESTIGATOR'S CHECKLIST

Conduct Preliminary Case Assessment

1. Does the patrol report adequately establish the PC 530.5 elements?
2. Have all the ID theft victims been identified and has contact information been provided?
3. Were there any victims besides the ID theft victims (such as merchants who were presented with forged checks or counterfeit credit cards)? Have they been adequately identified and has contact information been provided?
4. Is any necessary evidence located in other California jurisdictions or in other states?
5. Have suspects been identified? Are there co-defendants, accessories or accomplices?
6. Was a computer or the Internet used in the scheme?
7. Was there any search or seizure before you received the case? Where is that evidence and what has been done with it to date?

Initial Activities

8. Obtain additional evidence
 - a. Collect and secure any documents or materials noted in the patrol report that were retained by the victim or other witnesses.
 - b. If suspect is known, evaluate PC for search warrant or residence and vehicle. Also determine if you can have pre-existing searchable probation terms.
 - c. If Internet was used, send a preservation letter for account registration, e-mail correspondence, web site visits, and other on-line activity associated with the suspect's account. Include non-disclosure request in letter. Secure search warrant for ISP account and the suspect's computer. (Obtain assistance from District Attorneys Office if required.)
 - d. Serve search warrants as appropriate.
 - e. Arrange for forensic examination of any seized computers.
9. Identify additional victims
 - a. Make inquiries to determine if suspect has been active in other jurisdictions; obtain and consolidate any related police reports.

- b. Use seized financial records, ISP data and other information sources to identify individuals and businesses that may have been defrauded through the suspect's use of ID theft documents.
- 10. Collect business records that document the "unlawful use" element of PC 530.5. Comply with Evidence Code section 1271 by documenting:
 - a. A "qualified witness" who can testify to the identity or the business record and the mode of its preparation,
 - b. That the record was made in the regular course of business, and
 - c. That the record was made at or near the time of the suspect's transaction with the business, and
 - d. That the sources of information used to create the record, as well as the method and time of preparation indicate trustworthiness.
- 11. Develop an interview plan and, if possible, interview suspects.
- 12. Develop an estimate of the total losses.
- 13. Determine how long the scheme has been in operation.
- 14. Develop a theory on what the suspects have done with the proceeds of the scheme.
- 15. Develop an overall case theory, describe a "big picture" of the scheme and explain how it worked.
- 16. Develop a list of chargeable violations and be prepared to present the proof of those crimes to the DA for a charging decision:
 - a. Grand theft?
 - b. Forgery?
 - c. Burglary?
 - d. Access Card Violations (PC 484e-i)? Conspiracy?
 - e. False Personation?
 - f. Other?
- 17. Collect any evidence needed to sustain enhancement allegations:
 - a. Crime-Bail-Crime allegations (PC 12022.1)
 - b. Excessive taking allegations (PC 12022.6(a)(1), 12022.6(b) 1203.45a), and 186.11,
 - c. Allegations regarding other priorable behavior (Strikes, thefts, prior imprisonment)
- 18. Collect evidence needed for high bail setting and bail motions pursuant to PC 1275.1. (Prevents jail from accepting any bail until after a noticed motion)
 - a. You must submit an affidavit alleging that you believe the suspect has no funds that were not feloniously obtained.

- b. The judge then signs an order and the defendant cannot be released until he proves that his bail money is clean.
- 19. For assistance, contact the REACT Task Force (408-494-7186) or the District Attorney's High-Tech Crime Unit (408-792-2888)

Identity Theft
Patrol Officer's Basic Guidelines

IDENTITY THEFT PATROL OFFICER'S BASIC GUIDELINES

Taking the Victim Report

Who takes the initial report?

You do. According to PC 530.6(a), an ID theft victim may make a report to the law enforcement where he or she lives or works.

What should your report include?

Identify the victim and/or reporting party/parties.

Specify which identifying information was unlawfully used.

Secure a specific and unequivocal statement that use of the ID was not authorized.

Eliminate the possibility of ID use by family or friends who may have presumed authority to use the ID.

Determine how and where the identifying information was used (i.e., to commit a fraud or theft, to open a credit account, to obtain employment, to conceal identity, etc.)

Inquire if a point-of-compromise is known.

Collect the available evidence from the victim and book it into evidence.

Ask the victim to collect and retain all not-yet-available documents related to the incident (credit reports, bills, etc.) until contacted by follow-up investigators.

Ask the victim to complete a PC 530.8 request (see "Identity Theft Victim's Request for Fraudulent Transaction/Account Information")

Determine if there are additional victims and attempt to contact them as well.

Where should your report be referred?

In addition to the usual inter-departmental routing, you should also forward a copy of your report to the agency that has jurisdiction where the theft or unauthorized use occurred.

If a suspect is known, refer a copy of your report to the agency where the suspect resides.

Victim Assistance

See: Know your Rights: California Identity Theft Victim Rights

Witnesses Other than Victims

Collect statements and contact information from all witnesses to the unauthorized use (e.g., in a retail transaction, determine which specific employee or sales clerk had contact with the suspect).

In business cases, identify the custodian of records and note contact information.

Identify and secure evidence

Conduct identification procedures as per your agency's policy

Determine if surveillance tapes exist and request copy as appropriate.

If in a suspect-controlled location, check for notebooks, computers and digital storage media, access cards, checks, and other ID documents that may be relevant.

Suspect Present or Contacted

Confirm Identity

Determine suspect's actual identity, residence address, telephone/cell phone numbers, etc. Obtain CDL info.

Suspect Interview (Subject to usual Constitutional procedures)

Identify accomplices, co-conspirators, and instrumentalities used by the suspect.

Determine how the identity information was obtained, and whether there was any claimed authority or permission to use the information.

Determine whether/where the suspect used the identity information in other locations or businesses.

Follow-up Investigation

See: Identity Theft Investigator's Checklist

Identity Theft Investigator's Checklist

IDENTITY THEFT INVESTIGATOR'S CHECKLIST

Conduct Preliminary Case Assessment

1. Does the patrol report adequately establish the PC 530.5 elements?
2. Have all the ID theft victims been identified and has contact information been provided?
3. Were there any victims besides the ID theft victims (such as merchants who were presented with forged checks or counterfeit credit cards)? Have they been adequately identified and has contact information been provided?
4. Is any necessary evidence located in other California jurisdictions or in other states?
5. Have suspects been identified? Are there co-defendants, accessories or accomplices?
6. Was a computer or the Internet used in the scheme?
7. Was there any search or seizure before you received the case?
Where is that evidence and what has been done with it to date?

Initial Activities

8. Obtain additional evidence
 - a. Collect and secure any documents or materials noted in the patrol report that were retained by the victim or other witnesses.
 - b. If suspect is known, evaluate PC for search warrant or residence and vehicle. Also determine if you can have pre-existing searchable probation terms.
 - c. If Internet was used, send a preservation letter for account registration, e-mail correspondence, web site visits, and other on-line activity associated with the suspect's account. Include non-disclosure request in letter. Secure search warrant for ISP account and the suspect's computer. (Obtain assistance from District Attorneys Office if required.)
 - d. Serve search warrants as appropriate.
 - e. Arrange for forensic examination of any seized computers.
9. Identify additional victims
 - a. Make inquiries to determine if suspect has been active in other jurisdictions; obtain and consolidate any related police reports.

- b. Use seized financial records, ISP data and other information sources to identify individuals and businesses that may have been defrauded through the suspect's use of ID theft documents.
- 10. Collect business records that document the "unlawful use" element of PC 530.5. Comply with Evidence Code section 1271 by documenting:
 - a. A "qualified witness" who can testify to the identity or the business record and the mode of its preparation,
 - b. That the record was made in the regular course of business, and
 - c. That the record was made at or near the time of the suspect's transaction with the business, and
 - d. That the sources of information used to create the record, as well as the method and time of preparation indicate trustworthiness.
- 11. Develop an interview plan and, if possible, interview suspects.
- 12. Develop an estimate of the total losses.
- 13. Determine how long the scheme has been in operation.
- 14. Develop a theory on what the suspects have done with the proceeds of the scheme.
- 15. Develop an overall case theory, describe a "big picture" of the scheme and explain how it worked.
- 16. Develop a list of chargeable violations and be prepared to present the proof of those crimes to the DA for a charging decision:
 - a. Grand theft?
 - b. Forgery?
 - c. Burglary?
 - d. Access Card Violations (PC 484e-i)? Conspiracy?
 - e. False Personation?
 - f. Other?
- 17. Collect any evidence needed to sustain enhancement allegations:
 - a. Crime-Bail-Crime allegations (PC 12022.1)
 - b. Excessive taking allegations (PC 12022.6(a)(1), 12022.6(b) 1203.45a), and 186.11,
 - c. Allegations regarding other priorable behavior (Strikes, thefts, prior imprisonment)
- 18. Collect evidence needed for high bail setting and bail motions pursuant to PC 1275.1. (Prevents jail from accepting any bail until after a noticed motion)
 - a. You must submit an affidavit alleging that you believe the suspect has no funds that were not feloniously obtained.

b. The judge then signs an order and the defendant cannot be released until he proves that his bail money is clean.

19. For assistance, contact the REACT Task Force (408-494-7186) or the District Attorney's High-Tech Crime Unit (408-792-2888)

Know Your Rights:
California Identity Theft Victim Rights



Know Your Rights: California Identity Theft Victims' Rights

Identity theft is taking someone's personal information and using it for an unlawful purpose, such as opening credit accounts or making charges on the victim's account.¹

If you are a victim of identity theft you have rights that can help you clear up your records and avoid paying debts you did not create.

- **You have the right** to file a police report of identity theft with your local police department or sheriff's office, even if the crime was committed elsewhere.² A police report of identity theft is the key to getting the benefit of the other rights listed below.
- **You have the right** to get copies of documents relating to fraudulent transactions or accounts created using your personal information.³
- **You have the right** to have information resulting from identity theft removed (blocked) from your credit reporting agency files.⁴
- **You have the right** to receive up to 12 free credit reports, one per month, in the 12 months from the date of the police report.⁵
- **You have the right** to stop debt collection actions related to a debt resulting from identity theft. Before resuming collection, the collector must make a good faith determination that the evidence does not establish that the consumer is not responsible for the debt.⁶
- **You have the right** to bring an action or assert a defense against anyone claiming a right to money or property in connection with a transaction resulting from identity theft.⁷

If you are a victim of criminal identity theft, which occurs when an identity thief creates a false criminal record in your name, you have additional rights.



CALIFORNIA OFFICE OF PRIVACY PROTECTION

- **You have the right** to an expedited proceeding in Superior Court for getting a judge's order finding that you are factually innocent. The judge may order the deletion, sealing, or labeling of records.⁸
- **You have the right** to be listed in the California Department of Justice's Identity Theft Victim Registry. This gives victims of criminal identity theft a mechanism for confirming their innocence.⁹

For more information on identity theft, including a Victim Checklist, go to www.privacy.ca.gov or call 1-866-785-9663.

This fact sheet is for informational purposes and should not be construed as legal advice or as policy of the State of California. If you want advice on a particular case, you should consult an attorney or other expert. The fact sheet may be copied, if (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the California Office of Privacy Protection, and (3) all copies are distributed free of charge.

¹ California Penal Code Section 530.5.

² California Penal Code Section 530.6.

³ California Penal Code Section 530.8; Fair Credit Reporting Act Section 609(e) [15 United States Code § 1681g].

⁴ California Civil Code Sections 1785.16(k), 1785.16.1, 1785.16.3, 1785.203(b); Fair Credit Reporting Act Section 605B [15 United States Code § 1681c-2].

⁵ California Civil Code Section 1785.15.3(b).

⁶ California Civil Code Section 1788.18.

⁷ California Civil Code Section 1798.93.

⁸ California Penal Code Section 530.6.

⁹ California Penal Code Sections 530.6-530.7.

**Requesting Information on Fraudulent Accounts:
A Guide for Identity Theft Victims**



Requesting Information on Fraudulent Accounts: A Guide for Identity Theft Victims

Both California and federal law give an identity theft victim an important right. This is the right to get copies of documents relating to fraudulent transactions made or accounts opened using the victim's personal information. The information can help law enforcement investigate the crime and can prevent repeated violations.

You may use the form provided with this Information Sheet to ask creditors or other businesses to give you copies of applications and other business records relating to transactions or accounts that resulted from the theft of your identity.

Working with Law Enforcement

When you file your police report of identity theft, the officer may give you a form to use to request information from creditors or other businesses. If the officer does not do this, you may use the form provided here. After you receive the documents from the business, give copies to the officer investigating your case.

Contacting a Creditor or Other Business

When you call a creditor or other business to report the identity theft, explain that you will be sending a request for applications and other business records relating to the fraudulent transactions or account. Ask where you should send your request and if any proof of your identity or affidavit of identity theft is also required.

Fraudulent Account Information Request Form

The form is provided to help you request the information from businesses. You are not required to use it. If you choose to use the form, make copies of it. Fill out one copy for each creditor or business. Send each creditor or business a completed and signed form. Enclose a copy of your police report of identity theft. If a business asked you to send proof of identity, send the proof or affidavit requested. Also enclose a copy of the federal and California laws provided with this Information Sheet.

**Identity Theft Victim's Request for Fraudulent
Transaction/Account Information**

IDENTITY THEFT VICTIM'S REQUEST FOR FRAUDULENT TRANSACTION/ACCOUNT INFORMATION

Made pursuant to § 609(e) of the Fair Credit Reporting Act (15 U.S.C. § 1681g), California Financial Code §§ 4002 and 22470, Civil Code § 1748.95 and Penal Code § 530.8.

TO: _____ FAX: _____

ACCOUNT NO.: _____ REFERENCE NO.: _____

FROM: _____

I am a victim of identity theft. I am formally disputing a transaction or an account that I have learned has been made, opened or applied for with you. I did not make this transaction or open or apply for this account and have not authorized anyone else to do so for me. You may consider this transaction or account to be fraudulent. Below is my identifying information. I have filed a report of identity theft with my local police department and a copy is attached. Under federal and California laws, creditors and other business entities must provide a copy of application and business transaction records relating to fraudulent transactions or accounts opened or applied for using an identity theft victim's identity.

A copy of the relevant federal and California law is enclosed. The victim is generally permitted to authorize your release of the account information to a specified law enforcement officer. I am designating the investigator listed below as additional recipient of all account information and documents. I authorize the release of all account documents and information to the law enforcement officer designated. I am requesting that you provide copies of the following records related to the disputed transaction or account:

- Application records or screen prints of Internet/phone applications
- Statements
- Payment/charge slips
- Investigator's Summary
- Delivery addresses
- Any other documents associated with the account
- All records of phone numbers used to activate the account or used to access the account

Name: _____ Social Security Number: _____

Address: _____

Phone: _____ Fax: _____

Employer: _____ Phone: _____

Designated Police Department: _____ Report No.: _____

Designated Investigator: _____

Signed: _____ Date: _____

ID Theft Affidavit

ID Theft Affidavit

Victim Information

- (1) My full legal name is _____
(First) (Middle) (Last) (Jr., Sr., III)
- (2) (If different from above) When the events described in this affidavit took place, I was known as _____
(First) (Middle) (Last) (Jr., Sr., III)
- (3) My date of birth is _____
(day/month/year)
- (4) My Social Security number is _____
- (5) My driver's license or identification card state and number are _____
- (6) My current address is _____
City _____ State _____ Zip Code _____
- (7) I have lived at this address since _____
(month/year)
- (8) (If different from above) When the events described in this affidavit took place, my address was _____
City _____ State _____ Zip Code _____
- (9) I lived at the address in Item 8 from _____ until _____
(month/year) (month/year)
- (10) My daytime telephone number is (_____) _____
My evening telephone number is (_____) _____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER
GOVERNMENT AGENCY

How the Fraud Occurred

Check all that apply for items 11 - 17:

- (11) ☐ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.
- (12) ☐ I did not receive any benefit, money, goods or services as a result of the events described in this report.
- (13) ☐ My identification documents (for example, credit cards; birth certificate; driver's license; Social Security card; etc.) were ☐ stolen ☐ lost on or about _____
(day/month/year)
- (14) ☐ To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

Name (if known)

Name (if known)

Address (if known)

Address (if known)

Phone number(s) (if known)

Phone number(s) (if known)

Additional information (if known)

Additional information (if known)

- (15) ☐ I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.
- (16) ☐ Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.)

(Attach additional pages as necessary.)

**DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER
GOVERNMENT AGENCY**

Victim's Law Enforcement Actions

- (17) (check one) I ☐ am ☐ am not willing to assist in the prosecution of the person(s) who committed this fraud.
- (18) (check one) I ☐ am ☐ am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.
- (19) (check all that apply) I ☐ have ☐ have not reported the events described in this affidavit to the police or other law enforcement agency. The police ☐ did ☐ did not write a report. In the event you have contacted the police or other law enforcement agency, please complete the following:

(Agency #1)

(Officer/Agency personnel taking report)

(Date of report)

(Report number, if any)

(Phone number)

(email address, if any)

(Agency #2)

(Officer/Agency personnel taking report)

(Date of report)

(Report number, if any)

(Phone number)

(email address, if any)

Documentation Checklist

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

- (20) ☐ A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.
- (21) ☐ Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

**DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER
GOVERNMENT AGENCY**

Name _____ Phone number _____ Page 4

- (22) ☐ A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Signature

I certify that, to the best of my knowledge and belief, all the information on and attached to this affidavit is true, correct, and complete and made in good faith. I also understand that this affidavit or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may constitute a violation of 18 U.S.C. §1001 or other federal, state, or local criminal statutes, and may result in imposition of a fine or imprisonment or both.

(signature)

(date signed)

(Notary)

[Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:

(signature)

(printed name)

(date)

(telephone number)

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER
GOVERNMENT AGENCY

Fraudulent Account Statement

Completing this Statement

- Make as many copies of this page as you need. **Complete a separate page for each company you're notifying and only send it to that company.** Include a copy of your signed affidavit.
- List only the account(s) you're disputing with the company receiving this form. **See the example below.**
- If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (**NOT** the original).

I declare (check all that apply):

- ☐ As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

Creditor Name/Address (the company that opened the account or provided the goods or services)	Account Number	Type of unauthorized credit/goods/services provided by creditor (if known)	Date issued or opened (if known)	Amount/Value provided (the amount charged or the cost of the goods/services)
Example Example National Bank 22 Main Street Columbus, Ohio 22722	01234567-89	auto loan	01/05/2002	\$25,500.00

- ☐ During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing address _____

Account number _____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER
GOVERNMENT AGENCY

Instructions for Completing the ID Theft Affidavit

INSTRUCTIONS FOR COMPLETING THE ID THEFT AFFIDAVIT

To make certain that you do not become responsible for any debts incurred by an identity thief, you must prove to each of the companies where accounts were opened in your name that you didn't create the debt. The ID Theft Affidavit was developed by a group of credit grantors, consumer advocates, and attorneys at the Federal Trade Commission (FTC) for this purpose. Importantly, this affidavit is only for use where a new account was opened in your name. If someone made unauthorized charges to an existing account, call the company for instructions.

While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it. If they do not accept the ID Theft Affidavit, ask them what information and/or documentation they require.

You may not need the ID Theft Affidavit to absolve you of debt resulting from identity theft if you obtain an Identity Theft Report. We suggest you consider obtaining an Identity Theft Report where a new account was opened in your name. An Identity Theft Report can be used to (1) permanently block fraudulent information from appearing on your credit report; (2) ensure that debts do not reappear on your credit reports; (3) prevent a company from continuing to collect debts or selling the debt to others for collection; and (4) obtain an extended fraud alert.

The ID Theft Affidavit may be required by a company in order for you to obtain applications or other transaction records related to the theft of your identity. These records may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement.

This affidavit has two parts:

- Part One — the ID Theft Affidavit — is where you report general information about yourself and the theft.
- Part Two — the Fraudulent Account Statement — is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to write to.

When you send the affidavit to the companies, attach copies (NOT originals) of any supporting documents (for example, driver's license or police report). Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them.

Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks. Delays on your part could slow the investigation.

Be as accurate and complete as possible. You may choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Print clearly.

When you have finished completing the affidavit, mail a copy to each creditor, bank, or company that provided the thief with the unauthorized credit, goods, or services you describe. Attach a copy of the Fraudulent Account Statement with information only on accounts opened at the institution to which you are sending the packet, as well as any other supporting documentation you are able to provide.

Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that it was received. The companies will review your claim and send you a written response telling you the outcome of their investigation. Keep a copy of everything you submit.

If you are unable to complete the affidavit, a legal guardian or someone with power of attorney may complete it for you. Except as noted, the information you provide will be used only by the company to process your affidavit, investigate the events you report, and help stop further fraud. If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party. Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

If you haven't already done so, report the fraud to the following organizations:

1. Any one of the nationwide consumer reporting companies to place a fraud alert on your credit report. Fraud alerts can help prevent an identity thief from opening any more accounts in your name. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

- Equifax: 1-800-525-6285; www.equifax.com
- Experian: 1-888-EXPERIAN (397-3742); www.experian.com
- TransUnion: 1-800-680-7289; www.transunion.com

In addition, once you have placed a fraud alert, you're entitled to order one free credit report from each of the three consumer reporting companies, and, if you ask, they will display only the last four digits of your Social Security number on your credit reports.

2. The security or fraud department of each company where you know, or believe, accounts have been tampered with or opened fraudulently. Close the accounts. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number, your phone number, or a series of consecutive numbers.

3. Your local police or the police in the community where the identity theft took place. Provide a copy of your ID Theft Complaint filed with the FTC (see below), to be incorporated into the police report. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check www.naag.org for a list of state Attorneys General.
4. The Federal Trade Commission. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC also can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws that the FTC enforces.

You can file a complaint online at www.consumer.gov/idtheft. If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438-4338); TTY: 1-866-653-4261; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. When you file an ID Theft Complaint with the FTC online, you will be given the option to print a copy of your ID Theft Complaint. You should bring a copy of the printed ID Theft Complaint with you to the police to be incorporated into your police report. The ID Theft Complaint, in conjunction with the police report, can create an Identity Theft Report that will help you recover more quickly. The ID Theft Complaint provides the supporting details necessary for an Identity Theft Report, which go beyond the details of a typical police report.

**DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER
GOVERNMENT AGENCY**