



Identity Theft and Reporting

Section: 1.403
Effective Date: October 28, 2011
Amended: February 9, 2017

1.403 IDENTITY THEFT & REPORTING

1.403.02 Background Information

- A. During the 2010 legislative session the Maryland Legislature passed an amendment to the Public Safety Article, Section 3-207 of the Annotated Code of Maryland which the Governor signed into law.
- B. In part, that amendment requires the Maryland Police Training and Standards Commission to develop, with the cooperation of the Office of the Attorney General, the Governor's Office of Crime Control and Prevention, and the Federal Trade Commission, a uniform identity fraud reporting form that:
 - 1. Makes transmitted data available on or before October 1, 2011, for use by each law enforcement agency of State and local government; and,
 - 2. May authorize the data to be transmitted to the Consumer Sentinel Program in the Federal Trade Commission.

1.403.04 MPCTC developed ID Fraud Reporting Form

- A. In response to this legislative mandate the Police Training and Standards Commission staff has developed, in cooperation with the Office of the Attorney General, the Governor's Office of Crime Control and Prevention and the Federal Trade Commission the Identity Fraud Reporting form.
- B. At its January, 2011 meeting the Police Training and Standards Commission approved this form, for distribution to all Maryland law enforcement agencies.
- C. As part of its discussion the Commission considered the reporting requirement set forth in Maryland Criminal Law - CR § 8~394 - Report which states in part:
 - 1. *Contact local law enforcement agency* - A person who knows or reasonably suspects that the person is a victim of identity fraud, as prohibited under this subtitle, may contact a local law enforcement agency that has jurisdiction over:
 - a. any part of the county in which the person lives; or
 - b. any part of the county in which the crime occurred.
 - c. *Preparation of report.* - After being contacted by a person in accordance with subsection (a) of this section, a local law enforcement agency shall promptly:
 - i. prepare and file a report of the alleged identity fraud; and
 - ii. provide a copy of the report to the victim.
- D. The Commission recognizes that a number of law enforcement agencies use agency specific field reporting forms for various crimes and incidents, some of which may be generated in the field by computer and recorded and or stored electronically. It also recognized the Identity Fraud form it developed may not be compatible with those electronic report writing protocols.
- E. *While the law does not require the use of the form developed by the Commission, the Commission urges law enforcement agencies to adopt this form or a suitable facsimile that allows the identity fraud data/information captured on the uniform report to be collected in a format that is suitable for transmission to other law enforcement agencies and to the Federal Trade Commission.*

1.403.06 Electronic Report Form

- A. An electronic copy of the form developed by the Commission is on the R Drive under the folder named ***Departmental Forms*** and called the ***Identity Theft – Uniform Reporting Form***.
- B. The staff of the Commission developing instructions on the subject of identity theft/fraud that is suitable for use either in an entry-level program or for in-service training purposes.
- C. These instructions are posted with the report form on the R Drive.

1.403.08 Paper Report Form

- A. The approved paper report form is found with all instructions on the following Annex Pages.

1.403.10 Report Required – No Exceptions

- A. At this time, a paper form **MUST** be completed and furnished the victim. There are no exceptions to the protocol to complete this report and provide the victim with a copy.

+++++

See appendix for instructions and copy of the required report.

**UNIFORM REPORT – IDENTITY FRAUD/THEFT
INSTRUCTIONS FOR COMPLETING FORM**

PAGE 1 - LINES # 1-2: Reporting Agency Identifiers.

PAGE 1 - LINE # 3: Agency Complaint/Case Number.

PAGE 1 - LINE # 4: Date report taken.

PAGE 1 - LINES # 5-11: Victim Identification – to be completed as indicated on form.

PAGE 2 - BLOCK # 12: Determine if document/information was stolen or lost.

PAGE 2 - BLOCKS # 13-14: To be completed as indicated on form.

PAGE 2 - BLOCK # 15: Determine HOW victim discovered theft/compromise occurred – check all that apply.

PAGE 2 - BLOCK # 16: Determine identity information/item compromised – check all that apply.

PAGE 3 - BLOCK # 17: Determine from victim if information/identity was used to:

- establish NEW account;
- use an EXISTING account;

★ Note: Use separate pages if multiple/additional accounts are involved.

**PAGE 4 - BLOCK # 18: Obtain a detailed narrative from victim to include as much of the information contained in BLOCK # 18 as possible.
Use additional page(s) if necessary.**

PAGE 5 - BLOCK # 19: Determine from victim the names/identities of any “potential suspect(s).

PAGE 5 - LINE # 20: To be completed as indicated on form.

PAGE 5 - LINE # 21: To be completed as indicated on form if known.

PAGE 6 - BLOCK # 22: Page to be given to victim as reference/resource:

★ Note: Reporting officer should explain options/recommended actions to the victim if necessary.

ANNOTATED CODE OF MARYLAND

CR § 8-304. REPORT.

(a) **Contact local law enforcement agency.** – A person who knows or reasonably suspects that the person is a victim of identity fraud, as prohibited under this subtitle, may contact a local law enforcement agency that has jurisdiction over:

- (1) any part of the county in which the person lives; or,
- (2) any part of the county in which the crime occurred.

(b) **Preparation of report.** – After being contacted by a person in accordance with subsection(a) of this section, a local law enforcement agency shall promptly:

- (1) prepare and file a report of the alleged identity fraud; and,
- (2) PROVIDE A COPY OF THE REPORT TO THE VICTIM.

UNIFORM IDENTITY FRAUD/THEFT REPORTING FORM		
LAW ENFORCEMENT AGENCY IDENTIFIERS/ADMINISTRATIVE INFORMATION		
1. AGENCY NAME:	2. REPORTING AGENCY ORI #:	
3. COMPLAINT/INCIDENT/REPORT #:	4. DATE REPORT TAKEN:	
VICTIM INFORMATION		
5. LEGAL NAME OF VICTIM AT TIME OF REPORT:		
_____ (last)	_____ (first)	_____ (middle)
6. DATE OF BIRTH: _____		
7. VICTIM CURRENT ADDRESS:		
_____ (STREET NAME/APARTMENT #)		
_____ (CITY)	_____ (STATE)	_____ (ZIP CODE)
8. TELEPHONE #:		
_____ (home)	_____ (work)	_____ (cell – optional)
9. “E” MAIL ADDRESS (recommended/not required)		

10. DRIVER LICENSE INFORMATION:

_____ (number) _____ (state of issuance)

11. VICTIM FULL LEGAL NAME AT TIME OF THEFT/DISCOVERY OF THEFT *IF DIFFERENT FROM ABOVE:*

_____ (last) _____ (first) _____ (middle)

PERSONAL INFORMATION - IDENTITY THEFT/COMPROMISE SUMMARY

12. **DOCUMENT/INSTRUMENT/INFORMATION:** _____ LOST _____ **STOLEN** _____
 Section: 1.403
 Active Date: October 28, 2011
 Amended: February 9, 2017
 _____ UNAUTHORIZED DISCLOSURE OF PERSONAL INFORMATION FROM **OTHER RECORDS:**

TYPE OF RECORD: _____

13. **DATE IDENTITY THEFT FIRST NOTICED/DISCOVERED:** _____
 AMOUNT OF **MONEY** SPENT TO DATE TO RESOLVE THEFT (ESTIMATE IF NOT SURE): \$ _____
 AMOUNT OF **TIME** SPENT TO DATE TO RESOLVE THEFT (ESTIMATE IF NOT SURE): _____
 (HOURS)

14. **LOCATION/ADDRESS IDENTITY THEFT/LOSS BELIEVED TO HAVE OCCURRED:**

 (STREET)

 (CITY) (COUNTY) (STATE) (ZIPCODE)
 IF COMMERCIAL ESTABLISHMENT – NAME: _____

15. **IDENTITY THEFT/COMPROMISE DISCOVERED HOW (CHECK APPLICABLE):**
 _____ SELF-INITIATED CREDIT REPORT CHECK
 _____ FRAUDULENT/UNAUTHORIZED ACCOUNT:
 _____ OPENED _____ USED
 _____ OVERDRAWN ACCOUNT
 _____ CREDIT REPORT FINDING BY FINANCIAL/OTHER INSTITUTION
 _____ NOTIFIED BY:
 _____ BANK/CREDIT UNION/OTHER TYPE OF FINANCIAL INSTITUTION
 _____ CREDIT CARD COMPANY/OTHER CREDITOR
 _____ BILL COLLECTION AGENCY/REPRESENTATIVE
 _____ INSURANCE COMPANY
 _____ UTILITY/TELEPHONE COMPANY
 _____ DENIED LOAN/CREDIT
 _____ ARRESTED/HAD WARRANT ISSUED/COMPLAINT FILED FOR CRIME DID **NOT** COMMIT
 _____ DRIVER'S LICENSE SUSPENDED FOR ACTS **NOT** COMMITTED
 _____ SUED FOR DEBT **NOT** INCURRED
 _____ DENIED EMPLOYMENT FOR FINANCIAL REASONS
 _____ THEFT OF MAIL/DIVERSION OF MAIL FROM ADDRESS
 _____ GARBAGE/RECYCLABLES GONE THROUGH
 _____ OTHER (DESCRIBE): _____

16. **TYPE OF IDENTITY INFORMATION/ITEM COMPROMISED (CHECK APPLICABLE TYPES):**

_____ SOCIAL SECURITY NUMBER	_____ UTILITIES/TELEPHONE RECORDS
_____ DRIVER'S LICENSE	_____ ATM/BANK CARD
_____ BIRTH CERTIFICATE/OTHER	_____ SAVINGS ACCOUNT
_____ RESIDENT ALIEN CARD	_____ CREDIT CARD
_____ PASSPORT	_____ CHECKING ACCOUNT

<p>EDUCATIONAL RECORDS</p> <p>17. HOW INFORMATION/IDENTITY WAS USED (CHECK APPLICABLE):</p> <p>PROFESSIONAL RECORDS/LICENSE _____</p> <p>INSURANCE RECORDS: _____</p> <p> MEDICAL _____</p> <p> OTHER (IDENTIFY TYPE): _____</p> <p> FRAUDULENTLY OPENED NEW ACCOUNT (fill in applicable information) _____</p>	<p>BROKERAGE/STOCK ACCOUNT</p> <p>COMPUTER: _____</p> <p> INTERNET PURCHASE _____</p> <p> FILES HACKED _____</p> <p> OTHER (PROVIDE INFORMATION): _____</p> <p> ATTEMPTED TO OPEN NEW ACCOUNT (fill in applicable information) _____</p> <p> FRAUDULENTLY OPENED NEW ACCOUNT (fill in applicable information) _____</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- DATE OPENED: _____
- TYPE OF ACCOUNT: _____

- COMPANY NAME: _____
 - ACCOUNT #: _____
 - AMOUNT OBTAINED/CREDIT LIMIT: \$ _____
- COMPANY ADDRESS: _____
- COMPANY PHONE #: _____
- COMPANY "E" MAIL ADDRESS: _____

- TYPE OF FRAUD/THEFT:
 - _____ CASH OBTAINED: \$ _____
 - _____ MERCHANDISE OBTAINED: \$ _____
 - _____ SERVICES OBTAINED:
 - _____ GOVERNMENT BENEFITS;
 - _____ MEDICAL SERVICES;
 - _____ OTHER: _____

- _____ **EXISTING** ACCOUNT:
 - _____ FRAUDULENTLY ATTEMPTED TO USE **EXISTING** ACCOUNT (fill in applicable information)
 - _____ FRAUDULENTLY USED **EXISTING** ACCOUNT (fill in applicable information)

- TYPE OF ACCOUNT: _____
- COMPANY NAME: _____
 - ACCOUNT #: _____
 - AMOUNT OBTAINED/CREDIT LIMIT: \$ _____
- COMPANY ADDRESS: _____
- COMPANY PHONE #: _____
- COMPANY "E" MAIL ADDRESS: _____
- ACCOUNT #: _____

- DATE(S) ACCOUNT WAS USED: _____
 - TYPE OF FRAUD/THEFT:
 - _____ CASH OBTAINED: \$ _____
 - _____ MERCANDISE OBTAINED: \$ _____
 - _____ SERVICES OBTAINED:
 - _____ GOVERNMENT BENEFITS
 - _____ MEDICAL SERVICES
 - _____ OTHER: _____

[LIST ADDITIONAL/MULTIPLE STOLEN/COMPROMISED ACCOUNTS ON SEPARATE PAGES]

VICTIM ACCOUNT/NARRATIVE OF HOW THEFT OCCURRED OR DISCOVERED & ACTION TAKEN

18. **DETAILED NARRATIVE FROM VICTIM – INCLUDE THE FOLLOWING INFORMATION IF APPLICABLE:**

- LOCATION IDENTITY THEFT/LOSS BELIEVED TO HAVE OCCURRED
- DESCRIPTION OF PERSONAL INFORMATION LOST/STOLEN/COMPROMISED:
 - OTHER/ADDITIONAL IDENTITY INFORMATION LOST/STOLEN COMPROMISED
- DETERMINE IF VICTIM AUTHORIZED ANYONE TO USE NAME/PERSONAL INFORMATION:
 - IDENTIFY AUTHORIZED USER
- DATE THEFT/COMPROMISE OCCURRED/DISCOVERED
- EXPLANATION OF HOW THEFT/LOSS/COMPROMISE WAS *DISCOVERED*
- EXPLANATION OF HOW ACCESS WAS GAINED TO IDENTITY INFORMATION (if known)
- WAS IDENTITY THEFT RESULT OF ANOTHER CRIME:
___ BURGLARY ___ STOLEN AUTO ___ ROBBERY ___ OTHER TYPE THEFT
- DATE/TIME *OTHER* CRIME OCCURRED:
 - INCIDENT # (if known)
- DESCRIPTION OF HOW PERSONAL INFORMATION WAS USED/FOR WHAT PURPOSE
- AMOUNT OF FINANCIAL LOSS (known at time of this report)
- IF INTERNET PURCHASE - WEBSITE ADDRESS/COMPANY
- NAME/TELEPHONE # OF COMPANY REPRESENTATIVE/INVESTIGATOR MAKING CONTACT
- DATE THEFT/LOSS REPORTED TO COMPANY/INSTITUTION
- VICTIM IDENTITY VERIFIED BY REPORTING OFFICER AT TIME OF REPORT:
 - METHOD USED: _____
- DETERMINE IF VICTIM IS WILLING TO ASSIST IN THE INVESTIGATION/PROSECUTION IF SUSPECT IS IDENTIFIED/ARRESTED/CHARGED:
___ YES ___ NO ___ NOT SURE AT THIS TIME
- DETERMINE IF VICTIM HAS FILED A REPORT WITH ANY OTHER LAW ENFORCEMENT AGENCY:
 - IF YES, NAME OF AGENCY/REPORT #: _____
- DETERMINE IF VICTIM HAS ADDITIONAL DOCUMENTATION TO SUPPORT THEFT/FRAUD CLAIM THAT MIGHT ASSIST IN INVESTIGATION
 - IF YES, IDENTIFY DOCUMENT: _____

NARRATIVE:

"POTENTIAL" SUSPECT INFORMATION

19. "POTENTIAL" SUSPECT IDENTIFIERS:

SUSPECT NAME/ALIAS: _____

SUSPECT ADDRESS: _____

SUSPECT TELEPHONE #: _____

SUSPECT RELATIONSHIP TO VICTIM: _____

METHOD USED TO OBTAIN IDENTITY ITEM (if known/suspected):

AUTHORIZATION BY VICTIM TO SUSPECT TO USE PERSONAL IDENTITY INFORMATION:
___ YES ___ NO

IF YES, TRANSACTIONS/CIRCUMSTANCES AUTHORIZED FOR (EXPLAIN):

OFFICER CONTACT INFORMATION

20. NAME/ASSIGNMENT/TELEPHONE # REPORTING OFFICER:

(NAME) (TELEPHONE #) (E MAIL)

21. NAME/ASSIGNMENT/TELEPHONE # OF FOLLOW-UP INVESTIGATOR (if known):

(NAME) (TELEPHONE #) (E MAIL)

VICTIM ASSISTANCE INFORMATION/CHECKLIST

An Identity Theft Report entitles an identity crime victim to certain important protections that may help the victim eliminate fraudulent debt and restore their credit to pre-crime status. It is recommended that the victim of the identity theft be provided with the following information after the Identity Crime Report has been completed.

Briefly describe the agency investigative process that occurs after an Identity Theft Report is completed.

22. **RECOMMENDED ACTION TO BE TAKEN BY VICTIM (CHECK APPLICABLE):**

- ___ BEGIN WRITTEN LOG OF ACTION TAKEN TO INCLUDE:
 - DATES/TIMES OF CONTACTS
 - NAMES/TELEPHONE # OF CONTACTS
 - SUMMARY OF ACTION NEEDED/TAKEN
 - RECORD TIME SPENT/EXPENSES INCURRED FOR CONTACT
 - CONFIRM IN WRITING ALL CONVERSATIONS REGARDING THEFT/FRAUD/COMPROMISE
 - MAINTAIN COPIES OF ALL CORRESPONDENCE/DOCUMENTS REGARDING THEFT
- ___ OBTAIN/REVIEW COPY OF CREDIT REPORT(S):
 - EQUIFAX (800-685-1111) www.equifax.com
 - EXPERIAN (888-397-3742) www.experian.com
 - TRANS UNION (800-680-7289) www.transunion.com
- ___ IDENTIFY ALL OPEN FRAUDULENT ACCOUNTS:
 - IDENTIFY FRAUDULENT ACCOUNT NUMBERS
 - IDENTIFY FRAUDULENT ADDRESSES/OTHER INFORMATION
- ___ NOTIFY ALL CREDITORS ABOUT IDENTITY FRAUD COMPLAINT:
 - AUTHORIZE ACCESS TO FRAUDULENT ACCOUNT INFORMATION FOR LAW ENFORCEMENT FRAUD INVESTIGATORS
 - DISPUTE STOLEN ACCOUNTS WITH CREDITORS
 - REQUEST CREDIT REPORTING AGENCIES BLOCK FRAUDULENT INFORMATION
- ___ PLACE FRAUD ALERT
- ___ PLACE CREDIT FREEZE
- ___ OBTAIN REPLACEMENT CREDIT ACCOUNTS WITH NEW ACCOUNT # FOR EXISTING COMPROMISED ACCOUNTS
- ___ NOTIFY AFFECTED CREDIT CARD COMPANY/BANK/FINANCIAL INSTITUTION
- ___ FILE COMPLAINT WITH FEDERAL TRADE COMMISSION (FTC):
 - COMPLETE ID THEFT AFFIDAVIT (1-877-438-4338) www.ftc.gov/idtheft
- ___ OBTAIN IDENTITY THEFT PASSPORT:
 - OFFICE OF MARYLAND ATTORNEY GENERAL:
 - IDENTITY THEFT UNIT (410-576-6491) www.IDTheft@oag.state.md.us
- ___ MONITOR CREDIT CARD BILLS FOR EVIDENCE OF FRAUDULENT ACTIVITY:
 - REPORT ACTIVITY IMMEDIATELY TO CREDIT GRANTOR
- ___ NOTIFY SOCIAL SECURITY ADMINISTRATION IF SS# HAS BEEN COMPROMISED:
 - (1-800-269-0271)
- ___ NOTIFY MOTOR VEHICLE ADMINISTRATION IF DRIVER'S LICENSE HAS BEEN LOST/STOLEN/COMPROMISED:
 - (1-800-950-1682)
 - APPLY FOR "V" RESTRICTION ON DRIVER'S LICENSE FROM MVA;
- ___ CONTACT LOCAL LAW ENFORCEMENT AGENCY IF IDENTITY HAS BEEN USED TO COMMIT CRIMINAL VIOLATIONS:
 - FILE APPROPRIATE ADMINISTRATIVE REPORT FOR MISIDENTIFICATION:
 - LOCAL STATE'S ATTORNEY'S OFFICE www.mdsaa.org
 - PRIVACY RIGHTS CLEARINGHOUSE:
 - (1-619-298-3396) www.privacyrights.org

[USE THIS PAGE AS A VICTIM ASSISTANCE CHECKLIST]

