Bernards Township Police Department

1 Collyer Lane, Basking Ridge NJ 07920
908-766-1122
Chief Timothy King

Fraud & Identity Theft Questionnaire

The Bernards Township PD Detective Bureau has received your complaint of fraud or identity theft. Please fill out this questionnaire and return it in order to assist with the investigation. The Bernards Township Police Department has limited jurisdiction for the majority of identity theft and fraud complaints. The Bernards Township PD Detective Bureau tracks and analyzes these complaints to identify any local source of identity theft or fraud. A detective will contact you if any further information is needed. You will be informed if the investigation results in an arrest or if individuals are charged in another jurisdiction.

PROCEDURES:

Contact the involved financial institutions and request copies of their documents.

Fill out this form and return it to the BTPD. Please print clearly. The completed form can be mailed, emailed to: fraud@bernardspd.org, or dropped off in person at the Bernards Township Police Department located at: 1 Collyer Lane, Basking Ridge, NJ, 07920.

Bernards Twp Police Case#:_____ Officer: _____

Your Full Name: _____

Address: _____

_____

Cell Phone#: _____ Home# _____

Date of Birth: _____/_____/_____ Social Security #: _____ - _____ - _____

Drivers License # _____

Email Address: _____

How were you made aware of the fraud or identity theft? (Contacted by bank, credit card company, credit statement etc.) *May use additional paper if necessary.

What date did you first become aware of the identity crime? _____

Please list all of the fraudulent activity that you are aware of, with location (i.e. vendor or store name) and addresses of where fraudulent application or purchases were made. Please try to list incidents in chronological order. You may attach a separate sheet of paper if needed.

Please explain *in your words*, how your identity was compromised and how you believe it was fraudulently used, even if you are not completely certain.

Are you aware of any of your documents being stolen, copied, or passwords that may have been compromised (i.e. stolen mail, credit cards, lost wallet, suspicious internet transactions)?

Please list all of your accounts with fraudulent activity.

Credit Card: Full Account Number:

Bank Name: Full Account Number:

_____ _____

_____ _____

_____ _____

_____ _____

_____ _____

Utility Company/Other: Full Account Number:

_____ _____

_____ _____

_____ _____

_____ _____

To the best of your knowledge, what identity crimes have been committed?

_____ Unauthorized purchase(s) made using my credit card(s)/ numbers(s).

_____ Opening a new credit card account(s) in my name.

_____ Opening utility and/or telephone account(s) in my name.

_____ Unauthorized withdrawals from my bank account.

_____ Opening new bank account(s) in my name.

_____ Unauthorized loan(s) in my name.

_____ Unauthorized access to my securities or investment account(s).

_____ Obtaining government benefit(s) in my name.

_____ Obtaining employment in my name.

_____ Obtaining medical service(s) or insurance benefit(s) in my name.

_____ Evading prosecution for crime(s) using my name.

_____ Check fraud using my name.

_____ Passport/visa fraud.

_____ IRS or Social Security Fraud.

_____ Other _____

Retracing your actions in recent months with regard to your personal information will assist in the investigation. What circumstances and activities have occurred in the last six months (include activities performed by you and on your behalf by a member of your family or friends).

_____ I carried my Social Security Card in my wallet or purse.

_____ I carried my bank account password(s), PIN or code in my wallet or purse.

_____ I gave out my Social Security Number. To whom? _____

_____

_____ My mail, wallet, or purse was stolen or lost. When, where? _____

_____

_____ My mail was held at a post office or collected by another.

_____ I went on vacation or traveled. When, where? _____

_____ I did not receive a bill. Type of bill, when expected? _____

_____ I sent payment that was not received. To whom, when? _____

_____ Service personnel were in my home. Who, when?_____

_____ I made purchases on the internet. What?_____

_____ I made a mail order or telephone purchase. Method of payment? _____

_____ A charitable donation was made. To who? _____

_____ I won a prize. From who? _____

_____ I completed a member application. To what organization?_____

_____ I applied for a loan, credit, etc. With who? _____

_____ I leased and/or rented a vehicle. From who? _____

_____ I opened a utility account. With who? _____

_____ I applied for a license, permit, etc. With who? _____

_____ My personal information was given to someone. Whom? _____

_____ I was contacted by someone from another country about inheritance or lottery winnings, etc. Who? _____

_____ Other reasons that might explain the identity theft: _____

_____

_____

Did you report the incident to your credit card company, bank or other financial institution about the most recent misuse or attempted misuse of your personal information?_____

If so, please provide the following: (If multiple institutions, please add information on a separate sheet of paper)

Name of bank or institution:_____

Name and contact information of investigator: _____

_____

Case number assigned by institution: _____

Have you contacted the following organizations and requested a "*Fraud Alert*" or "Credit Freeze" to be placed on your account(s)?_____

☐ Equifax (800)378-4329

☐ TransUnion (800)916-8800

☐ Experian (888)397-3742

☐ Federal Trade Commission http://www.identitytheft.gov/#/

☐ Others (Please list) _____

☐ FBI Internet Crimes Complaint Center: https://complaint.ic3.gov/

☐ Have you requested a copy of your credit history?

☐ Was money sent through any (P2P) money transfer applications (e.g., Zelle, Cash App, Venmo, PayPal, Apple Cash/Pay, Google Pay, etc.). If so, please list all transaction dates and times, amounts, tokens (emails and telephone numbers money was sent to), and bank accounts. Also provide all transaction ID #'s if available. Use additional paper if necessary.

_____

_____

_____

_____

_____

_____

_____

_____

_____

Wires:

_____ Were funds wired? If so, please provide all receipts with wire transaction details from your bank. Immediately call your bank to have wire(s) recalled. *Important - Victim must immediately file a report with the FBI's IC3 Website: **https://complaint.ic3.gov/**

Date/Time	Recipient Bank Info	Amount

Make a copy of this document for your records.

I declare under penalty of law that the information I have provided is true and correct to the best of my knowledge. Knowingly submitting false information on this form could subject you to criminal prosecution.

Name: Date:

_____ _____

Signature:

_____

Supplemental Information

Protect Yourself

Recognize scam attempts and end all communication with the perpetrator. The perpetrators will try to keep you on the phone for the duration of the scam or until you make the requested payments to discourage you from calling family, friends, and police.

Search online for the contact information (name, email, phone number, addresses) and the proposed offer. Other people have likely posted information online about individuals and businesses trying to run scams.

Resist the pressure to act quickly. Scammers create a sense of urgency to produce fear and lure victims into immediate action. Call the police immediately if you feel there is a danger to yourself or a loved one.

Be cautious of unsolicited phone calls, mailings, and door-to-door services offers.

Never give or send any personally identifiable information, money, jewelry, gift cards, checks, or wire information to unverified people or businesses.

Make sure all computer anti-virus and security software and malware protections are up to date. Use reputable anti-virus software and firewalls.

Disconnect from the internet and shut down your device if you see a popup message or locked screen. Pop-ups are regularly used by perpetrators to spread malicious software. Enable pop-up blockers to avoid accidentally clicking on a pop-up.

Be careful what you download. Never open an email attachment from someone you don't know and be wary of email attachments forwarded to you.

Take precautions to protect your identity if a criminal gains access to your device or account. Immediately contact your financial institutions to place protections on your accounts. Monitor your accounts and personal information for suspicious activity.

A utility company will never ask you to pay your utility bill using wire transfers or ask for immediate payments utilizing PayPal, Venmo, or Zelle.

Never pay someone requesting money with gift cards!

Common Fraud Schemes

Romance scam: Criminals pose as interested romantic partners on social media or dating websites to capitalize on their elderly victims' desire to find companions.

Tech support scam: Criminals pose as technology support representatives and offer to fix non-existent computer issues. The scammers gain remote access to victims' devices and sensitive information.

Grandparent scam/Bail scam: Criminals pose as a relative—usually a child or grandchild—claiming to be in immediate financial need. **Don't Become A Victim**

- **Verify** that it is your grandchild by contacting their parents and additional family members or asking a question only your real grandchildren would know the answer to.
- **Resist** pressure to send money quickly and secretly.
- **Refuse** to send immediate payments utilizing wire transfers, girft cards, overnight delivery, and all (P2P) money transfer applications (e.g., Zelle, Cash App, Venmo, PayPal, Apple Cash/Pay, Google Pay)

Government impersonation scam: Criminals pose as government employees and threaten to arrest or prosecute victims unless they agree to provide funds or other payments.

Sweepstakes/charity/lottery scam: Criminals claim to work for legitimate charitable organizations to gain victims' trust. Or they claim their targets have won a foreign lottery or sweepstake, which they can collect for a "fee."

Home repair scam: Criminals appear in person and charge homeowners in advance for home improvement services that they never provide.

TV/radio scam: Criminals target potential victims using illegitimate advertisements about legitimate services, such as reverse mortgages or credit repair.

Family/caregiver scam: Relatives or acquaintances of the elderly victims take advantage of them or otherwise get their money.

Utility company scam: Criminals target victims and threaten to cut off service unless an overdue bill or maintenance cost is paid immediately.

How to Report

If you believe you or someone you know may have been a victim of fraud, contact your local police department. You can also file a complaint with the FBI's Internet Crime Complaint Center(IC3).

When reporting a scam, regardless of dollar amount, include as many of the following details as possible:

- Names of the scammer and/or company provided to you.
- Dates/Times of all contact.
- Methods of communication and methods of payments received or made.
- Phone numbers, email addresses, mailing addresses, and websites used by the perpetrator.
- Details where you sent funds including wire transfers, all P2P applications, and bank accounts. Provide bank names, account names, and account numbers.
- Descriptions of your interactions with the scammer and the instructions that you were given.
- Keep all original documentation including emails, text messages, social media instant messages, phone logs & messages, bank statements, all bank correspondence, faxes, and logs of all other communications.