DISTRICT ATTORNEY'S OFFICE

Anthony M. Matulewicz III, District Attorney
NORTHUMBERLAND COUNTY COURTHOUSE
201 MARKET STREET
SUNBURY, PENNSYLVANIA 17801
PH# 570-988-4134 / FAX 570-988-4135

PRESS RELEASE

Date: 23 March 2023

To: All Media Outlets

Re: Credit Card Debt - Settlement Scam

Details:

1. The District Attorney's Office encountered an elaborate and well developed scam in which a company identifying itself as **Waverly & Associates** (purported to be based in **Los Angeles, California**), attempted to scam a 65 year old Coal Township woman in a credit card related matter.

2. The aforementioned business, operating as a mediation service for the Bank of America, claimed an alleged credit card debt of $12,000.00 could be immediately settled for $ 3,200.00 if paid by the end of the day. This scam started with a phone call to the resident who then provided an e-mail address to the scammer.

3. The letter subsequently e-mailed to the victim was professionally written and contained all of the information that would be expected in an authentic notice. At the time of initial contact, the scammer already possessed the full social security number of this resident, lending credibility to the scheme. The caller spoke in English, was articulate, and no foreign accent was detected.

4. An investigation by the District Attorney's Office revealed this was a scam attempt. The only initial clue of a scam attempt was the request for immediate payment. It is important to remember that scammers impose a sense of urgency in nearly all scams, giving victims less time to think about the actions they are taking.

5. If you are contacted by anyone and urged to make an immediate payment or you are threatened with arrest or incarceration, you are likely involved in a scam attempt. The phone number appearing in your caller ID can be "spoofed" and should never be trusted to confirm the source or identity of any caller.

6. Never provide your social security number, driver's license number, or financial account information to any caller unless you are certain the transaction is legitimate. It is also best to avoid storing photocopies of this information on your cell phone, or in your e-mail accounts. If you must keep copies on your phone or computer, store this information in a reputable password manager or encrypted container.

7. Use strong passwords on all accounts and activate multi-factor authentication (commonly referred to as 2FA) in all applications that provide it.

Tony Matulewicz
District Attorney