MAIL FRAUD/CHECK WASHING

What is it?

While many forms of fraud are relatively new, mail fraud has long been a favorite tactic by fraudsters to steal from businesses and individuals.

Generally, this involves the criminal gaining access to legitimate checks in various ways:

- ✔ Checks left in residential mailboxes overnight or for long periods of time
- ✔ USPS blue collection boxes after the last pickup time
- ✔ Burglary of USPS facilities
- ✔ Robbery of USPS employees
- ✔ Bribery and/or collusion of USPS employees

Once they are in possession of the stolen checks, fraudsters will usually either utilize “check washing” or “check cooking” to redirect money into accounts they control.

How It’s Done

CHECK WASHING

- ✔ Fraudster uses chemicals to physically alter the check
- ✔ Typical ways checks are altered are by changing the original Payee or by changing both the Payee and the amount

CHECK COOKING

- ✔ Fraudster digitally manipulates the image of the stolen check using readily available photo editing software and high-tech printers
- ✔ Fraudster manufactures multiple checks from the single check image
- ✔ Checks are often written for smaller amounts which often go undetected for longer periods of time by escaping the scrutiny of larger check amounts

Avoid Being a Victim

- ✔ Use e-check, ACH automatic payments and other electronic and/or mobile payments.
- ✔ Use mobile or online banking to access copies of your checks and ensure they are not altered. While logged in, review your bank activity and statements for errors.
- ✔ If your bank provides an image of a paid check, review the back of the check to ensure the endorsement information is correct and matches the intended payee, since criminals will sometimes deposit your check unaltered.
- ✔ Use pens with indelible black ink so it is more difficult for a criminal to wash your checks.
- ✔ Don’t leave blank spaces in the payee or amount lines.
- ✔ Follow up with payees to make sure that they received your check.