

# PREVENTING FRAUD

## Verify Personal Information When Processing New Accounts

- Consult independent sources such as a phone directory, the applicant's credit report or employer, or software for verifying consumer information.
- Check for inconsistencies in information such as a ZIP code that fails to match the street address or telephone area code.
- Make sure **all** the required information is given before processing an application.

## Check the Applicant's Other Accounts for Fraudulent Activity

---

The applicant's credit report will contain a **fraud alert** if one or more of the applicant's accounts has been a target of fraud. The alert will provide information for contacting the victim.

Do not process the application or extend credit until you have contacted the individual or have used other means to independently verify the applicant's identity.

Other signs of possible fraudulent activity include:

- Numerous credit inquiries in a short period of time.
- A recent pattern of late payments in the absence of a history of such payments.
- Higher than normal credit balances.
- A recent change of address in conjunction with other suspicious signs.

## Verify Requests for Changes of Address

---

If within 30 days of receiving a change of address notification for a credit or debit card account, your institution receives a request for an additional card or a replacement card, it must verify the change of address in one of the following ways:

1. Send a notice to the cardholder's former address; provide a way for the cardholder to promptly report an incorrect address change.
2. Notify the cardholder using any other agreed-upon method; provide a way for the cardholder to promptly report an incorrect address change.
3. Use other means approved by your identity theft policies.

If the address change was verified before an additional card or a replacement card was requested, no address change verification is required.