Expertise Support Accuracy Efficiency

CREDIT COMPLIANCE

AUTHORIZATIONS

- Authorizations should always be on company letterhead.
- Authorizations must be signed and dated by both parties when doing a joint report before credit is pulled. Credit cannot be pulled on both unless both signatures are dated on the same day the credit file is pulled.
- Authorizations must be retained on file for two years.

PHONE REQUEST FORMS

- Credit files that are pulled with only a verbal phone request should have a Phone Request Form filled out with the consumer's information dated and signed by the person taking the personal information.
- A security question should be asked as evidence of the applicant's approval for the lender to obtain their credit file. Please document the answers to the security questions in your loan file. Examples of security questions:
  - What is your mother's maiden name?
  - What street did you live on while in grade school?

LOGONS AND PASSWORDS

- Logons and Passwords should not be shared. If there is a fraud, the person whose logon and password that is used will be the responsible party.

DATA SECURITY

- All employees that are terminated for any reason should have their logon and password locked or deleted immediately by their administrator.

ENCRYPTION

- Consumer personal information should never be emailed unless encrypted. Information can be faxed or should be downloaded into our system with their work order.

SECURITY BREACHES

- Security breach of any type concerning the consumer's personal information and/or credit file report should be reported immediately to United One Resources.

PERMISSIBLE PURPOSE

- Credit files should not be pulled for any other reason other than the Permissible Purpose the customer is set up for. For example if set up for Mortgage they cannot pull on that same account for Home Equity, Auto Loans, Personal Loans, Tenant Screening, etc. Each Permissible Purpose needs a separate set up.