**Large Withdrawal Loss Prevention Questionnaire Guidance**

Considerations before utilizing this Questionnaire

1. If there is any question regarding your customer’s ability to make decisions on their own behalf, if the customer is under extreme duress, or the bank is aware of mental or medical issues affecting the customer, please seek legal counsel before using this questionnaire.

Purpose of this Questionnaire

1. Encourage your customer to consider the negative impacts of completing the transaction.
2. Documented proof the bank counseled their customer. The number of lawsuits filed by victim consumers against their financial institutions is growing. If the trend continues, financial institutions will need documented proof a customer was counseled prior to completing the requested transaction.

When to use this Questionnaire

1. When there are concerns regarding a customer’s out-going transaction, such as:
   1. Unusually large cash withdrawals (this could be a safety risk as well)
   2. Wire transfer requests to an unusual party (cryptocurrency exchange) or for an unusual purpose (investing in a foreign business)
   3. Requests to purchase a Cashier’s Check but the customer doesn’t seem to know the payee (has to read information on their phone or from a printed paper)

|  |  |
| --- | --- |
| Purpose for your request: | Bank staff should pay attention to the customer’s stated purpose for the funds.  Does the purpose make sense for the customer?  If the purpose is questionable – ask more questions and/or take the matter to a supervisor for review.  If, after completing the questionnaire, the customer insists on completing the transaction:  *Cash Withdrawal* – Based on your institution’s practices, seek supervisor review or complete the transaction as requested.  *Cashier’s Check Purchase* payable to another party – Make sure the customer understands they can only file a claim for reimbursement of a lost, stolen or missing Cashier’s Check, if the check has not been negotiated in 90 days. Caution customer against providing a photo or digital image of the check to the intended payee or any other party.  *Wire Transfer* – the bank has the right to refuse to conduct a wire transfer if the wire transfer may be facilitating fraudulent activity. |
| **READ ALOUD** | **Providing fully candid and truthful responses to these questions will help us do our best to protect you and your assets.** |
| Are you **currently on the phone** with someone guiding you through this request?  If yes, please answer with a gesture – head shake or thumbs up. | If the customer indicates they are on the phone with someone:   * Signal or quietly ask them to hang up * Signal or quietly ask them to leave their phone/earbuds on your desk/counter * Move the customer’s phone/earbuds to a quiet, secure area of your desk/counter where the listener can’t hear * Motion for the customer to follow you to another room where the party on the other end can’t hear the conversation * Politely ask your customer questions about what is going on. |
| Were you told **not to tell anyone** the purpose of your withdrawal? | If the customer response is Yes:   * Politely ask them to tell you the story of what is going on.   If the customer response is No:   * Kindly remind your customer that providing fully candid and truthful responses helps you assist them.   If the withdrawal is from a recently funded loan or other credit:   * Ask more questions or talk to the loan officer!!  Although the customer may have sufficient collateral to support the loan, they risk losing that collateral when they can’t sustain the payments. * If the funds are from a recent unusual credit (ACH, wire, P2P), ask more questions. The customer may be acting as a Money Mule (see below). |
| Have you been told to provide a **false reason** for your withdrawal such as purchasing a car or remodeling at your home? | Bank staff should pay attention to the customer’s stated purpose for the funds, especially on requests for large cash withdrawals:  If the customer already drives a newer vehicle or states the funds are buying a vehicle for a relative/friend, please ask more questions. What kind of vehicle or who are they buying the vehicle from? Any hesitation in answering the question may indicate coaching from a scammer.  If the customer says they are remodeling their house, kitchen, or bathroom, does your customer own their home, how old is the home, who is the contractor conducting the work, is the contractor someone local or can they be paid with a cashier’s check.  Ask the customer if they are taking the cash to deposit into a cryptocurrency ATM (see below).  Make sure the customer understands leaving the bank with a large sum of cash is also a security risk. |
| Did someone you have **never met in person** or someone you **haven’t seen in a very long time** ask you to send them money? | Most scams are conducted via the internet, including social media.   * If your customer has never met the requestor in person where they could touch them, the risk of victimization doubles. * If the initial communication came from a social media post, text, or email from someone they know, ask them to call that person before completing the request. |
| Were you recently instructed to **purchase gift cards**? | Many scams start with asking someone to purchase a lower value pre-paid gift card as a test before asking for a larger amount. If the customer followed instructions on gift card purchases and sending the card information, they will probably follow instructions for sending a larger amount in another payment form. |
| Has anyone asked to **connect to your computer or mobile phone**? | If the customer reports they’ve allowed someone who is not a party to their account(s) to connect to their computer or mobile phone, take immediate actions to protect the customer’s access to internet/mobile banking services.   * Check for any unusual internet/mobile banking log-in activity. If found, suspend access pending further review. * Review account activity for unusual debits or transfers. If found, suspend account(s) and cancel debit cards until protective or recovery actions can be initiated. |
| Have you recently talked to a **government official** who is demanding money to avoid arrest, deportation, fines, to pay unpaid taxes, or **your bank** to secure your accounts or help with a criminal investigation of an employee? | Law enforcement agencies in the United States **do not** call people prior to arrest or deportation! They just show up with a warrant.  The Internal Revenue Service **does not** take tax payments over the phone, in cash, or with gold.  Your financial institution **will not** tell you if an employee is being investigated for theft of customer funds or other criminal activity.  Financial institution regulators/inspectors **do not** tell customers when an institution is on the brink of failure.  The United States government **does not** confiscate purchases of gold, silver, or other precious metals for safe keeping. |
| Did you recently receive a deposit from someone you don’t know and need to **withdraw the funds to send to someone else**? | The taking and re-distributing of fraudulently obtained funds, at someone else’s direction, is a form of money laundering. The person conducting these transactions is termed as a “Money Mule”.  This type of activity can lead to felony criminal charges.  <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/money-mules> |
| Were you recently told you won a **lottery or sweepstakes** but need to pay taxes or fees first? | Politely ask if the customer purchased a lottery ticket or entered a sweepstakes contest. When did they purchase/enter?  In the United States, all taxes and fees are withdrawn from the proceeds. Payment of any expenses is not required prior to winnings distribution.  If the customer indicates they won a foreign lottery or sweepstakes, please advise, they must travel to that country to accept their winnings. |
| Did you receive an **urgent call** from a family member who is in trouble or injured? | Scammers will always say “do not tell anyone”.  Call the family member before sending money. If no answer, call another family member to confirm the situation.  Attorneys and jailers **do not** take payment by gift card, gold or CashApp/Venmo! |
| Were you told to take cash to deposit into a **bitcoin/cryptocurrency ATM**? | ATMs offering the purchase of bitcoin/cryptocurrency have become the criminals’ choice for receiving funds.  Legitimate businesses and government agencies will not take payment through cryptocurrency ATMs.  Investing in cryptocurrency requires a strong understanding of how cryptocurrency works. If your customer doesn’t understand it, they should not rely on someone else to guide them through the process.  Once the cash is put in the ATM machine, recovering funds is nearly impossible. |
| Are you withdrawing these funds because you are being **harassed or threatened**? Is something **bad** going to happen if you don’t complete this transaction? | If you are being harassed or threatened, please call your local law enforcement immediately.  If something bad is going to happen to someone else if you don’t complete this withdrawal, please take a minute to think through the situation or call the AARP Fraud Watch Network Helpline at **877-908-3360** (you do not have to be a senior or member of AARP). |

Give the customer a copy of the signed document and information on common scams. The bank should retain the original or a scanned copy of the original according to bank policy (we suggest 2-3 years).

Banks using this questionnaire and guidance are free to add or remove content to fit their institutions practices. Considerations include:

* Employee response if the customer refuses to sign the form or leaves the institution without taking their customer copy.
* Retention period for signed forms
* How many times can a customer be counseled before management intervention is needed

2024 Oklahoma Bankers Association