***NOTICE****: The following has been provided by WBA committee and section volunteers for use by member banks.   
It should be reviewed and revised as appropriate to the user-bank’s own policies, procedures, and practices.*

**INTRODUCTION TO SECURITY**

The safety of employees and customers is a priority of Bank. There are established policies, procedures and processes in place to protect you, our customers and the bank. You will learn about the security threats we face and how you should handle these situations.

**Why it’s important**

As you may already know, there are many threats a bank faces. These threats range from robberies to online fraudulent transactions. In your role as a teller, you have the ability to prevent these situations. If the proper precautions are not taken, it could result in physical or mental harm to you, your customers or the bank; as well as a possible financial loss to your customers and the bank. Being alert to your surroundings and using precaution when processing every transaction is the first step to ensuring the safety of all.

**Emergency Situations**

When you think about security in a bank, your mind may first go to robbery. This is just one emergency situation in a bank, and you will learn there are several others that are just as dangerous. This matter should not be taken lightly; knowing how to handle these situations is vital to everyone’s safety. Below you will find an introduction to the different types of situations you might encounter and how you should handle them.

**Robbery**

One of the most threatening situations at a bank is a robbery. The most important thing you can do to prevent a robbery, other than following the established security procedures, is to be alert to your surroundings. Make eye contact and greet all customers entering the lobby. Attentive employees are the biggest deterrence for a robber.

You can never completely prevent a robbery, so you must know how to handle the situation if your branch is robbed. For the safety of everyone, the most important thing to do is comply with the robber and remain calm.

G*uidelines to follow in a robbery situation:*

* Cooperate and remain calm.
* Observe the suspect’s appearance and mannerisms.
* Retain the holdup note and/or other evidence if possible.
* Include bait money (if safe to do so).
* Set off the alarm as soon as it is safely possible.
* The doors should be locked immediately after the robber leaves to keep them from reentering the bank and to keep others out in order to preserve the crime scene.
* Notify the most senior staff member in the branch after the robbery has occurred. They will use the Robbery Response Kit to distribute the Post Robbery Assignment Cards to other staff members.
* Close your teller window and lock up your cash supply.
* Avoid touching your teller area or anywhere else the robber may have touched and do not allow anyone else to enter your area.
* Complete an Ident-A-Form.
* Stay in the building, but do not discuss details of the robbery with anyone until you have been debriefed by law enforcement.
* Do not answer any questions from the media, only an authorized spokesperson may do so.

**Bomb Threats**

Criminals create bomb threats to cause an evacuation of the bank, giving them easy access to funds. Do not allow unauthorized personnel in any restricted areas and be alert for suspicious looking people with packages. If you receive a bomb threat you must take it seriously, no matter how ridiculous or false it may seem. Notify your supervisor or the most senior staff member in the branch immediately if you are suspicious of anyone in the branch.

**Kidnapping and Hostage Situations**

Criminals may kidnap a bank associate or their family members and take them hostage. It is important all bank employees have an up to date Employee Personal Profile form on file with Corporate Security. This form contains information about you, your family members and your routine whereabouts. It will provide law enforcement with background information that could be helpful to the investigation.

Some precautions you can take to prevent a kidnapping or hostage situation are:

* Be aware of your surroundings as you are driving to and from work.
* Do not take the same route home from work every day.
* Walk around your car before entering it to ensure there is nobody under or inside of it.
* Don’t allow any strangers to enter your home.
  + Be especially wary of strangers who appear to be in “trouble.”
  + Request ID from any service or maintenance personnel to verify they are supposed to be at your home.
* Do not give out your personal information.
* Avoid indications that you are not home.
* Taking extra caution with your children since you work for a financial institution.

If you ever become part of a kidnapping or hostage situation, it is most important to remain calm and do exactly as you are told!

**Fire**

In the event of a fire, your first concern should be people’s safety – your own, your customers and your coworkers. If you have time before evacuating the building, place cash, checks, and deposits in your cash drawer and return it to the vault. If you do not, place all your teller work in your drawer and lock your cash drawer before leaving your window. Do not take your cash drawer outside of the teller or vault areas. Be sure to follow the fire and evacuation procedures outlined for your building.

**Dual Control**

We have already discussed dual control in previous lessons, but now we will focus on the locks and combinations. As you will recall, dual control requires two bank employees to complete a task or transaction. Both persons involved in the transaction or task are held accountable if there are any discrepancies. As a teller, there will be multiple times throughout the day that you will need to complete a task in dual control. It is important to remember that these tasks are required to be done under dual control for a specific purpose; to protect customers, the bank and yourself.

**Locks and Combinations**

You will be assigned specific combinations or keys that will be used in conjunction with another bank employee’s combination or key to open the branch vaults. *Never* share your combination or key; this means keeping your half in your possession or a secure place at all times. Copies of combinations in a sealed envelope and spare keys will be kept in a designated locked area in the branch and can only be accessed under dual control if they are ever needed. If you have a number combination, it is important you do not allow the other person to read your combination (if it is written down) or to closely observe you as you input the combination.

If you share your half of a combination with an associate who has the opposite half, this puts the bank at risk for possible embezzlement and you and the other employee at risk of termination. As you should recall from previous lessons, you will also be assigned teller drawer keys, these should always remain in your possession and not be shared with anyone. If you are ever asked to share your combinations or keys, report this to your supervisor or the branch manager immediately. If it is your supervisor or branch manager requesting your combination or key, report this to your regional manager immediately. You will also want to notify Corporate Security in this type of situation.

**Fraud**

Detecting fraudulent transactions will protect your customers and the bank from a financial loss. As technology advances, the type and complexity of fraudulent transactions are ever-changing. Criminals are even able to do many types of fraudulent transactions from the comfort of their own home. It is important you take the necessary precautions for every transaction you process and become familiar with your customer’s routine transactions. In order to protect your customers from fraud, you should question any transaction that is out of the ordinary from their normal transactions. As always, refer to your supervisor if you do not feel comfortable processing the transaction.

**Identity Theft**

Identity Theft is the fastest growing crime in the United States, therefore protecting customer information is more important than ever. In your role you have the opportunity to educate your customers on how they can prevent Identity Theft.

Below, you will find a list of ways you and your customers can prevent Identity Theft:

|  |  |
| --- | --- |
| **You (the teller)** | **Your Customer** |
| Shred all documents with customer information. | Safeguard your personal property. Your Social Security number is the key to your identity, keep it in a secured location at all times. |
| Keep all customer information at your teller window out of the view of other customers. | Shred all personal information, including incoming mail. Also, all outgoing mail should go through a secured post box. |
| Positively identify customers and confirm they have authorization on the account before giving out any information. If you have *any* doubts, don’t give out the information. | Be aware of your surroundings as you are filling out account information or are entering your PIN when using your debit card. |
| Do not allow any customers to approach your teller window or stand too close when you are processing another customer’s transaction. | Online Banking customers- Do not share your password and install virus software on your home computer. |
| Educate your customers on how to prevent Identify Theft. | Store all account and personal information in a secure place. |
| If you suspect your customer is a victim of Identity Theft contact their relationship manager. | Do not provide any identifying information unless you initiated the request or it is truly necessary. |

**Types of Teller Fraud**

You will learn about many types of fraudulent transactions you will encounter at the teller line. To give you a brief overview of the types of fraudulent transactions, a sample list has been compiled for you:

|  |  |
| --- | --- |
| **Type of Fraud** | **What is it?** |
| **Credit and Debit Card Fraud** | Using an unauthorized card to obtain goods or money. |
| **Counterfeiting** | Producing, using or selling counterfeit credit or debit cards, checks, monetary instruments or cash. |
| **Forgery** | Signing as the maker or endorser, filling in, altering or erasing bank documents such as checks or withdrawal slips. |
| **Con Artist** | Someone who swindles by deception or fraud. |
| **Check Kiting** | The manipulation of negotiable instruments to create artificial balances at a financial institution. |
| **Fast Change Artist** | Ask for change and then quickly suggest other denominations while trying to confuse or distract you in hopes you will lose your concentration and give out more change than you should. |
| **Embezzling** | The fraudulent misuse of bank funds or depositor’s money by a bank associate. |
| **Mysterious Disappearance** | Unexplained disappearance of money or negotiable instruments from the bank. |
| **Computer Intrusion** | Gaining access to the bank computer system to steal bank or customer information or to affect critical systems of the bank. |
| **Social Engineering** | Individual posing as a bank customer in order to obtain confidential customer information. |
| **Processing Personal and Family Member Transactions** | You are prohibited from processing your own, family member’s or close friend’s transactions in case of any discrepancies that may put you at risk. |