***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.*

**Counterfeit Checks 101**

**Fake Check Scam Overview:**

Fake check scams continue to target customers and are evolving. Unfortunately, most victims have little-to-no ability to repay their bank when their account becomes overdrawn. Many scams purportedly involve work from home job assignments, automobile wrap advertising, overpayments on items listed for sale, contest winnings, romance scams, and legal settlements. Although scams may differ, the anatomy remains the same. If someone sends a customer a check to deposit with instructions to send money back—it’s always a scam. It is crucial that our staff be familiar with these scams in order to minimize losses.

Fraudsters often seek out victims through robocalls, email solicitations, online job boards, classified advertising, and various social media platforms. Some even purchase lists of people who were previously scammed to target them for other offers.

The victim is convinced to deposit a check to their account themselves or are tricked into providing their online banking credentials to someone else to make the deposit. Cleverly, a fictitious balance is created in the victim’s account. Once the funds are made available, the victim is instructed to send most of the funds elsewhere.

Although traditional methods of conducting withdrawals at the counter or by ATM work well, fraudsters are using other electronic payment methods such as Cash App, Venmo, Zelle, PayPal, and Bitcoin to get their money faster before the bank realizes that the check is fake. After the funds are liquidated, the check is returned unpaid – overdrawing the account.

Fraudsters generally use accurate information from compromised business accounts like a bank’s ABA, account number, and approximate check range to produce fake checks. Moreover, it’s not uncommon to see fake cashier’s and official checks in circulation too. In other words, the checks will usually meet basic negotiability standards and are designed as an attempt to fool even experienced bank staff. With that in mind, it’s important to recognize red flags such as:

* A recent check deposit that appears much higher than expected.
* The check is issued from an out-of-state or unfamiliar financial institution.
* The check appears to be printed on generic looking stock.
* The back of the check contains a preprinted mobile deposit endorsement and/or the endorsement looks forged.
* Unusual memo lines such as “instant cash”, “direct deposit”, “advance”, or “approved”.
* The maker listed on the check doesn’t appear to have a logical connection to the customer.
* The customer is concerned when funds will be “available”.
* The customer was instructed to send money to someone else shortly after the deposit.

Although fake checks can be created using any amount, the amounts often seen range from $1,200 to $4,900. Fake checks can be deposited at the branch by the customer, or by mobile deposit. However, some checks are mailed directly to a branch with instructions to deposit the item to the victim’s account.

When in doubt, it’s best not to accept the check and follow your bank’s procedures on suspicious account activity.

**Operation Homeless – Branch Fraud:**

Business check cashing fraud, dubbed “operation homeless” by law enforcement, continues to impact our industry. Furthermore, it can negatively affect customer perception when fraudulent “on-us” checks are cashed at your bank.

Although there are many kinds of check fraud schemes, business check cashing fraud begins when a customer’s legitimate business checks are taken from commercial mailboxes. The compromise often occurs when a customer’s outgoing mail or the recipient’s mailbox is breached. These mailboxes are often unsecured – making them an ideal target to steal checks. Once the checks are stolen, the ringleader produces quality counterfeit checks that closely resemble the features of legitimate checks. In this type of fraud, the intent is to cash as many checks as possible at numerous bank branches – sometimes pocketing tens of thousands in just one day.

The ringleader creates the checks, but recruits individuals (mules) to cash the checks if they have current and valid identification. In turn, the mules receive a small portion each time a check is paid out. In an organized fashion, these criminals travel around the state with counterfeit items, drawn on many accounts from different banks.

Fortunately, there are ways to stop fraud in its tracks. Here are some suggested best practices for front-line staff:

* Compare the check to recently cleared checks as well as the signature card on file.
* Look for signs of traced, forged, or scanned signatures that appear irregular.
* The current check range on recently cleared items may be considered, however a counterfeit check is often in the current range.
* Look for recently issued identification (sometimes mules will obtain identification for the sole purpose of committing check fraud).
* Refuse to cash the check when presented with worn or damaged identification that omits information.
* Refuse identification that doesn’t appear to match the individual presenting the check.

Be aware of some common red flags that may be indicators of business check cashing fraud such as:

* The branch location is “out of the way” from the person presenting the check’s address listed on the check or listed on the identification presented.
* The person presenting the check came to the branch on foot or was dropped off.
* The person presenting the check appears anxious, rushed, overly chatty, or name drops.
* The person is in contact with someone on their mobile phone while the transaction is being performed.

To help mitigate your institution’s risk of loss, it is recommended that checks presented by non-customers be handled with additional scrutiny. Most importantly, if the maker of the check does not have positive pay services, consider adopting procedures where an authorized signer is contacted to validate checks over a certain dollar amount.

**Original Content:**

There are a lot of ways a person can get scammed out of their money. There are descriptions of a lot of check scams that you might find helpful. Part 1 describes the original Nigerian scam that has been around for a long time. The scam originated years ago in Nigeria where corruption and lack of law enforcement have created a safe haven for this type of activity. Organized crime groups in Nigeria employ hundreds of people who work long hours in public Internet cafés scamming United States citizens. These groups are pulling in millions of dollars annually from unsuspecting victims overseas. The Nigerians have adapted to newer technology and do use email now instead of letters and faxes. You can now find large Nigerian populations in Great Britain and Canada.

Nigerian 419 Scam:

This is the original scam from which all the others have developed. This scam involves the victim receiving a letter, fax, or email from someone claiming to be a high-level government official from a foreign country, commonly Nigeria. Sometimes they claim to be the wife of a high-ranking government official that has died or been killed. The individual tells the victim that they have a large sum of money, often from a U.S. contract with their country that they and their associates would like to invest in the United States. They seek the assistance of someone with a U.S. bank account to assist them to get the money into the country in exchange for a percentage of the money. If the victim agrees to help, they will be asked to wire money to pay expenses or to bribe officials to release the money. If the victim does not have the money, they will often be sent a check that they are instructed to cash or deposit and then wire the money (usually via Western Union or Money Gram). Of course, the check is counterfeit and comes back after the money has been wired. This scam can escalate to huge sums of money if the victim wires the “bribe money” from their own funds. This signals that the customer has money and can likely deposit a larger check without raising suspicion.

Inheritance Scam:

This scam evolved from the original 419 scam and has many of the same characteristics. As in the 419 scam, the victim receives a letter, fax, or email from someone overseas, but this time they are writing to inform the victim that a long lost relative has died or been killed. The departed relative has substantial assets in the foreign country that they have left to the only surviving heir, the victim. From here the scam follows the 419 scenarios as attorney fees and such must be paid to claim the inheritance. If the victim does not have the means to pay the fees, they are put in touch with someone who will loan them the money. The loan comes in the form of a counterfeit check. Again, these scams have the potential to evolve into very large sums of money.

Internet Auction Scam:

Everybody loves e-Bay, including the scammers! This scam evolved from the 419 scam, but because it involved lower dollar amounts and new technology, had a much higher percentage of success for the scammer. In this scam, the victim places an item for sale on the Internet (not necessarily on e-bay, often on local classified websites). The winning bidder contacts them to arrange payment, but there is a catch. The buyer is overseas, and shipping needs to be arranged. Payment is sent in the form of a counterfeit check for thousands of dollars in excess of the purchase price. The buyer is asked to wire the excess money to the buyer’s shipper who will arrange pickup of the item (they are often told that there is a little extra money for them to keep for their trouble to sweeten the deal). The money is wired before the check comes back, leaving the victim (or their bank) out the money.

Lottery Scam:

This is now the most popular of the counterfeit check scams, probably because of the high level of success that the scammers have had with it. It is also very difficult to detect because the checks are usually lower dollar amounts (less than $3,000 in most cases). The victim will receive a letter or email notification informing them that they have won a lottery or sweepstakes. Originally, it was either the Canadian Lottery or the El Gordo Lottery in Spain; however, now they are using any manner of sweepstakes or lottery including the Publisher’s Clearing House. They are given a counterfeit check to finance the taxes and fees associated with collecting the prize. They are asked to cash or deposit the check and wire the money to an individual who is collecting the “tax”. The reason this is so successful is that it plays on an American dream. Also, most times there is a contact phone number that the person can call, of course it is the scammer on a non-traceable cell phone who is safely outside the U.S. The victims are also told not to disclose their good fortune until they collect their grand prize. The scammers have seemingly plugged all the holes in their other scams with this one and it is very successful.

Work from Home Scam:

Another very effective counterfeit check scam is the work from home scam. In this scam, the scammer places ads on job search sites or replies to those who post job wanted ads. Once hooked up with a victim, the scammer gives the details of the work. The scammer claims to be a foreign company that needs assistance in collecting their accounts receivable from their U.S. clients. All the victim is required to do is receive checks, deposit them, keep a percentage for themselves, and forward the rest of the funds via wire to their employer. Obviously, the checks are counterfeit and the victim or their bank is left holding the bag.

Mystery Shopper Scam:

A variation on the work from home scam in which the victim is to be a “mystery shopper.” They are sent a counterfeit check and instructed to use the funds to complete several transactions, the largest of which is a Western Union wire transfer and evaluate the service they receive. Of course, the wire is sent to the scammer and the customer is left stuck with the bad check. This scam puts some pretty tight time frames for completion and urges the victim to keep their assignment secret from everyone. They have also printed fake bank phone numbers on the face of the check.

Charitable Organization Scam:

This is where the scammers sink to some of their lowest levels. They will surf the message boards of Christian organizations and gain the trust of an unsuspecting victim. They will claim to be a born-again Christian who has a large sum of money that they want to invest in a Christian church or organization. From here it evolves into the 419 scam where money is needed to bribe government officials to facilitate the transaction.

Lonely Hearts Scam:

This is one of the saddest of all the counterfeit check scams. In this one, the scammers surf personal ads or matchmaking websites for unsuspecting victims. They befriend someone and become involved in a cyber relationship. Once the victim is hooked, the scammer says that they want to come to the U.S. to be with them. They ask for money to fly to the U.S. and if the victim cannot or will not send it, they are sent a counterfeit check from a “relative” of their overseas companion which they are asked to cash and forward to them for a plane ticket.

**Some Things to Look for on Counterfeit Items:**

* The MICR number line on the bottom of the checks is not printed with real MICR ink. MICR ink is very dull, and the edges are very clean and sharp. MICR numbers on counterfeits are generally slightly shiny and not as sharp as real checks. Not using MICR ink is an advantage for the scammer because the check is not automatically read by sorting machines and increases the clearing time.
* Counterfeit checks are generally printed on lower quality ink jet printers instead of laser printers. Also, items that appear to be embossed may not have the raised print of real embossing.
* These checks are printed on real check stock so all the security features you would expect can and will be present on them. Real check stock is readily available in office supply stores.
* Signatures on counterfeit items can often be a tip off. English is not the first language of most of these scammers and they are not comfortable printing or writing without the aid of a computer. Signatures may often be printed on the check from a scanned copy of an American signature. These will often have a “digitized” look to them. If the item is signed by hand, the signature may appear scribbled and may contain many up and down pen strokes.
* Prominent phone numbers printed on the face of the check may be there to bait the victim or the bank into calling the number to verify the check. Often the phone numbers go directly to the scammer.
* Counterfeit checks often come to the victim via Fed EX or UPS overnight. If they come in the mail, they often will have Canadian postage stamps or cancellations. If Nigerian postage is on the envelope, you can be assured that you have a counterfeit. Scammers sometimes will get around this by sending the check to a third party in the U.S. to be forwarded to the victim.
* A letter that contains poor English and spelling will often accompany counterfeit checks.