Counterfeit Check Scams 101

One of the largest risks to U.S. banks as far as fraud loss goes is counterfeit check scam. These scams originated several 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 us citizens. These groups are pulling in millions of dollars annually from unsuspecting victims overseas.

Originally, these groups would contact their victims via letter or fax then lure them to their country where they would kidnap them and hold them for ransom. Now with the availability of computers and Internet access, things have become much easier.

Some of these groups have left Nigeria to work in other parts of the world such as the UK and Canada. Many other foreign organized crime groups have also copied the scams originally developed by the Nigerians.

In addition to the danger of our customers receiving counterfeit checks as part of these scams, we also need to be aware of another very real threat. Personal and Business customers who deal with individuals or companies located outside the U.S. are at risk of having their account information compromised and used to create counterfeit items that are sent to unsuspecting victims of these scams. If these items are paid by our bank and later found to be counterfeit – we take the loss. Scammers who work in their mailroom and make photocopies of checks received from U.S. companies have infiltrated companies in Canada. These copies are used to create counterfeit checks used in the scams we are about to discuss.

While we will be discussing the most common types of these scams, there are no hard fast rules here. The scams are always evolving and we see new twists all of the time. We rely heavily on our front line people to be alert to unusual circumstances and to ask questions of their customers. Explaining to a customer that we have seen a lot of counterfeit check fraud and do not want them to become a victim can usually overcome any objections they may have to your questions.

Common Scenarios Where Customers Receive Counterfeit Checks

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 e-mail 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 e-mail 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 e-mail 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 himself 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 of 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 adds 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 of 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.

As you have probably noticed, while the scenarios in which the victim is roped in are different and often change and evolve, the final part of these scams are all the same. The victim receives a counterfeit check and is asked to forward the funds outside the U.S. via Western Union, Money Gram, or some other money transfer service.

Types Of Counterfeit Checks

Washed or Altered Checks: - This is how the original scams were conducted. The scammers would get canceled checks from legitimate U.S. bank accounts and use simple chemicals to wash away the original payment information and the cancellation stamp. Sometimes they would actually just erase the information from the front of the check with an ink eraser. These were fairly easy to detect and were usually a long shot for the scammer.

Counterfeit Cashier's Checks and Money Orders: - With the increasing availability of cheap PC's, printers, check printing software, and check stock counterfeit checks took a huge leap forward. Now scammers are not reliant on making alterations to an existing check, they can print their own. If you are going to print your own checks, why not make them cashier's checks or money orders? These items have maximum hold periods mandated by Reg. CC that are far too short for the checks to clear, meaning that the funds have to be made available to the victim before the checks can be returned. The scammers know this and use it to their advantage, as well as the fact that many Americans still believe that cashier's checks and money orders are as good as cash. These checks can usually easily be verified by calling the bank on which they are drawn. To counteract this, the scammers have actually started placing their own phone numbers in place of the bank's phone number on the checks.

Counterfeit Company Checks: - These checks are a little bit trickier to deal with and are becoming more common as cashier's checks are being scrutinized more. They are checks that appear to come from legitimate U.S. companies ranging from furniture manufacturers to insurance companies. The checks usually contain the actual routing number and account number of the company's real bank account, so if you call the bank to verify the check they will often tell you that the check is good. The only way to actually verify these checks is to track down the actual phone number of the company and speak with their accounts payable department. Again, don't rely on numbers printed on the check or supplied by the scammer or victim.

Counterfeit U.S. Treasury Checks: - These are less common as they are a bit trickier for the scammer to pull off, but not impossible with a scanner and good color printer. They are relatively easy for experienced bankers to pick out, but some are pretty good. The treasury has a toll free number 1-804-697-2605 to verify treasury checks. Also, there is a set of 4 digits encoded in the bottom of all treasury checks (the last 4 encoded numbers) that represent the month and year the check was issued. These numbers always match the month and year of issue at the top of the check for a genuine U.S. Treasury Check.

Counterfeit U.S. Postal Service Money Orders: - These items are easy to pick out if you compare them to a real U.S. Postal Service Money order. Buying a genuine postal service money order for $0.01 to keep on the teller line is a good idea. Counterfeits are often issued for the maximum amount and are several are presented at once. The U.S. Postal Service will verify their money orders at this toll free number 1-866-459-7822.

Canadian or International Checks: - Be very careful with checks that are drawn on Canadian or foreign banks that are not payable through a bank in the U.S. Checks that are payable through Canadian or foreign banks are not subject to U.S. banking regulations and can take over a month to be returned. The only way to protect yourself and the customer when accepting these items is to send them for collection. This involves mailing the item directly to the bank and requesting guaranteed

funds in return before the customer's account is credited.

Counterfeit Traveler's Checks: - These are likely the least common of the counterfeit items because they are the most difficult to create. Also, it is fairly uncommon for an individual to receive a traveler's check from a third party.

Some Things To Look For On Counterfeit Items:

- The MICR numbers 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 of the security features you would expect can and will be present on them.

- 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.

- Sometimes the customer will provide their account information to a scammer in order to receive a wire transfer. The scammer will then send a counterfeit check via Fed EX or other overnight service to a branch office of their bank with a letter to deposit the check to the customer's account. When the customer checks their balance, they believe they have received the wire and move forward with the scam.

None of these rules are a sure thing. The scenarios and methods are always changing. The only way to combat this is to be alert for non-local items and be familiar with what is normal for

your customer. Also be careful about accepting checks that exceed the available balance in the account without placing holds.

Here are some check verification numbers you may find useful.

Counterfeit Check Verification Numbers

Travelers Express:
Cashier's Checks 1-800-323-6873
Money Orders 1-800-542-3590
(Some Travelers Express items will say "Payable Through U.S. Bank, St. Paul MN" in the bottom or upper left hand corner)

Bank of America:
Cashier's Checks 213-240-6374
Regular Checks 818-707-2699

Wells Fargo:
Cashier's Checks 480-394-3122

Integrated Payment Systems (IPS):
Cashier's/Official Checks
and Money Orders with 9 digit serial # 1-800-223-7520

Money Orders with 11 digit serial # 1-800-999-9660

Citi Bank: 302-323-5062

U.S. Postal Service Money Orders: 1-866-459-7822
U.S. Treasury Checks: 1-804-697-2605

Chase Bank Fraud Hotline: 1-800-727-7375