Oak Bank

You can't be the best, if you're only the same!

SECURITY UPDATE - SEPTEMBER 2021

Don't keep those documents, shred them instead!

Back in the office? Still working from home? It's best practice to create systems to keep documents safe. You should separate business and personal files before shredding them. By doing this, you'll prevent fraud and protect your personal information.

In California vs Greenwood, the U.S. Supreme Court implied that anyone can go through your trash, stating that the "expectation of privacy in trash left for collection in an area accessible to the public…is unreasonable."

Generally, identity theft is a crime of convenience; thieves will avoid any theft that requires a lot of effort. Identity thieves are unlikely to target properly shredded documents as they are difficult to piece together. It is best to shred your documents using a cross-cut method so that thieves can't tape the strips together again.

One item most people don't think about shredding is junk mail, and the consequences can be dangerous. Most people don't realize it, but junk mail usually has a computer barcode on the front that can sometimes contain personal identifying information. Pre-authorized credit card offers, mail from insurance companies and lenders, and even mail from associations and other membership organizations may have your personal information. You should shred all of your junk mail, including the return envelopes provided.

Where should my documents go?

Safeguard your documents by locking them up in a safe or a lockable container that can't easily be accessed. Documents shouldn't be kept for too long. Create a filing system to determine which documents have shorter retention periods and which ones need to be kept for longer.

What else should you shred?

- Address labels from junk mail and magazines
- ATM receipts
- Bank statements
- Birth certificate copies
- Canceled and voided checks
- Credit and debit card bills, carbon copies, summaries and receipts
- Credit reports and histories
- Documents containing your maiden name (used by credit card companies for security reasons)
- Documents containing names, addresses, phone numbers or email addresses
- Documents relating to investments
- Documents containing passwords or PIN numbers
- Driver's licenses or items with a driver's license number
- Employee pay stubs
- Employment records
- Expired passports and visas
- Unlaminated identification cards (college IDs, state IDs, employee ID badges, military IDs)
- Legal documents
- Investment, stock and property transactions
- Items with a signature (leases, contracts, letters)
- Luggage tags
- Medical and dental records
- Papers with a Social Security number
- Pre-approved credit card applications
- Receipts with checking account numbers
- Report cards
- Resumés or curriculum vitae
- Tax forms
- Transcripts
- Travel itineraries
- Used airline tickets
- Utility bills (telephone, gas, electric, water, cable TV, internet)

Oak Bank will never make unsolicited telephone requests or send emails asking for your personal information, password or other sensitive data.

If you have any questions, concerns or suspect you've been a victim of a scam, please call 608.441.6000.

*For additional security information you can visit **Oak Bank's Security Information** on our website.*