

Identify Suspicious Activity

Routinely monitor your banking accounts and billing statements and be alert to signs that require your attention on any of the following:

- Bills that do not arrive as expected
- Denials of credit for no apparent reason
- Unexpected credit card or account statements
- Calls and letters about purchases you did not make
- Inspect your credit reports, your accounts, and bill payment history closely
- Keep an eye on your bank and credit card statements for transactions you did not make. Place a call to your bank or Credit Card Company if needed.



Toll-Free 866-892-1LSB (1572)

Website LakesideBank.com

Mortgage Loans **312-567-0501**

Lakeside Link-Telephone Banking 312-939-BANK (2265)

To report lost or stolen cards 877-849-5533

Board of Trade

141 W. Jackson Blvd. Chicago, IL 60604

North Loop

55 W. Wacker Dr. Chicago, IL 60601

Chinatown/Pilsen

2200 S. Archer Ave. Chicago, IL 60616

South Loop

1350 S. Michigan Ave. Chicago, IL 60605

Lakeview/Lincoln Park

2800 N. Ashland Ave. Chicago, IL 60657

UIC/Near West

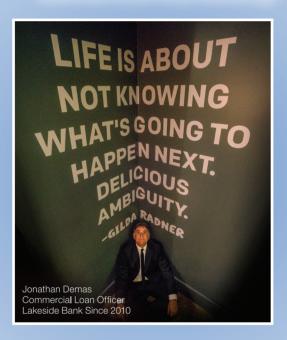
1055 W. Roosevelt Rd. Chicago, IL 60608

Elmhurst

165 S. York St. Elmhurst, IL 60126

Privacy & Security

Unpredictable Can Be Good— But Not With Your Security











Prevent Identity Theft

It's important to stay ahead of identity theft. There are constant risks. Be informed and talk to your Lakeside Banker for more suggestions or if you have questions about any suspicious account activity.

- Shred financial documents and paperwork with personal information before you discard them.
- Protect your Social Security number. Keep your Social Security Card out of your wallet and do not write it on any checks or pieces of paper. Unless it's absolutely necessary, avoid giving your Social Security number to anyone or any organization. Ask about using another form of identification.
- Don't give out personal information over the phone, mail, or internet unless you know exactly who you are dealing with.
- Never click on links sent in unsolicited emails. Trusted firewalls, anti-spy ware, and anti-virus software may serve as useful tools to protect your computer.
- Avoid short and obvious passwords! Do not use personal information, such as your name name, mother's maiden name, pet's name, birthdates, or the last four digits of your Social Security number.
- ▲ Keep personal information secure at home, specifically if you employ outside help.

Identify Suspicious Activity

Place a "Fraud Alert" on your credit report and renew the reports carefully. The three nationwide consumer reporting companies have toll free phone numbers for placing an initial 90-day free fraud alert:

Equifax Experian TransUnion 800-525-6285 888-397-3742 800-680-7289

Placing a fraud alert entitles you to a free credit report. The alert stays in your file for at least 90 days and an extended report stays for 7 years. To place either alert you must provide proof of your identity. For more information about the identity theft report visit: www.ftc.gov.

- To obtain consumer resources and find out how to protect yourself from ID Theft, visit: www.idtheftinfo.org.
- Close all accounts that may have been tampered with.
- To obtain the ID Theft Affidavit, go to www.consumer.gov/idtheft.
- Keep copies of documents and records of your conversations, name of the person you spoke with, and their phone number.
- Report the theft to the Federal Trade Commission. Your report helps law enforcement across the country in their investigations (www.ftc.gov).

This Notice Is Required By Law

You have the right to a free credit report from www.AnnualCreditReport.com or 877-322-8228, the only authorized source under the Federal Law.

More Ways To Be Protected

- Enroll in an Identity Protection Program that can provide insurance, monitoring, and an Identity Theft Restoration service.
- Stop receiving credit card solicitations at home. Opt out of pre-screened credit card services by calling 1-888-567-8688.
- Enroll in internet banking for up to date info on your accounts.
- Ask your credit card companies, bill pay service, or utility companies to receive paperless statements.
- Enroll for online access on all your credit cards to monitor charges periodically.

Common Ways Theives Steal Your Identity

- Dumpster Diving: They rummage through trash looking for bills or other paper with your personal information.
- Skimming: They steal credit/debit card numbers by using a special storage device when processing your card.
- Phishing: They pretend to be financial institutions or companies and send spam or pop-up messages to your email to get you to reveal your personal info.
- ▲ Changing Your Address: They divert your billing statements to another location by completing a "change of address" form.
- "Old-fashioned" Stealing: They steal wallets and purses, and mail. They steal personal records from their employers or bribe employees who have access.