Consumer Laws

Illinois and federal laws that help protect you as a consumer

July 2023

Illinois General Assembly

Commission on Government Forecasting and Accountability

Commission on Government Forecasting and Accountability

Co-Chairperson	Senator David Koehler
Co-Chairperson	Representative C.D. Davidsmeyer
Executive Director	Clayton Klenke
Deputy Director	Laurie Eby

SENATE	*HOUSE*
Omar Aquino	Sonya Harper
Donald DeWitte	Elizabeth Hernandez
Elgie Sims	Martin McLaughlin
Win Stoller	Anna Moeller
Dave Syverson	Joe Sosnowski

Commission on Government Forecasting & Accountability
802 Stratton Office Building
Springfield, Illinois 62706
Phone: 217.782.5320
Fax: 217.782.3513
http://cgfa.ilga.gov

Consumer Laws

July 2023

Revised by David Miller, Research Administrator,
and other members of the CGFA research staff

Publication 564

Introduction

This booklet describes Illinois and federal laws that are meant to protect you as a consumer. The discussion is by subject, sometimes using a question-and-answer format. Topics addressed include online security, avoiding scams, checking your credit history, preventing or recovering from identity theft, and making major purchases, with suggestions by experts on ways to protect yourself.

Numbered endnotes, shown on the last pages of the booklet, list each law or other source mentioned in the text. You can use those endnotes to look up laws online or at many public libraries for more information. The final section of the booklet's text has contact information in case you need to enforce consumer rights.

Modern electronic communications make consumer transactions easier than ever. Unfortunately, they sometimes can enable bad actors to steal your money or personal information. This booklet can help you stay safe when shopping, borrowing, and buying.

Clayton Klenke
Executive Director

Contents

Doing Business Online or by Phone

The "snake oil" sellers of yesteryear have been replaced by a far larger number of dubious electronic sellers today. Everyone who uses electronic devices to do business should know the dangers of fraudulent activity. Major ways to avoid becoming a victim are described below.

Stopping unwanted solicitations

How can I stop phone and text solicitations?

The Federal Trade Commission (FTC) has a national "Do Not Call" Registry—a list of phone numbers that commercial telemarketers must not call. You can register your number(s) at www.donotcall.gov or (888) 382-1222.[1] Registration is permanent unless you ask to be de-registered. Some kinds of calls to registered numbers are still legal. They include charitable solicitation calls, political calls, and calls from companies with which you did business in the last 18 months.[2]

The Do Not Call list cannot stop all scammers. Many are abroad and cannot be prosecuted. So you still need to be wary of calls and texts from strangers. If you have registered your number, and a caller—not of an exempt type—tries to get you to spend money, it is almost surely a scam. (See "*Common kinds of scams*" on page 5 for more on scam calls and messages.)

Protecting accounts from intruders

Cybercriminals constantly try to enter financial, email, and other accounts to get money, or personal information they could use to get it. Keeping them out requires strong security measures. Major ones are described below.

General Computer and Mobile Device Security

There is no foolproof shield against online threats. But these actions will make you much less vulnerable:

(1) Keep your operating system and other software up to date.

Many cyberattacks exploit software flaws that were found, and for which corrective "patches" were issued, months or even years before. Thus it is critically important to keep your software up to date. Operating systems and applications usually can be set to update automatically, or to notify you when a security patch is issued. Immediately downloading and installing updates will go far to protect you against attacks.

(2) Use good security software.

Having up-to-date device software is essential; but you also need security software. (You might think of up-to-date device software as a door lock, and security software as a burglar alarm.) New computers typically have pre-installed security packages from one of the companies that offer it. After a trial period, you can pay to keep using it, or buy other security software. No security software can block all new threats. But there are websites that compare how effectively each brand of security software found known threats in tests.

Web browsers typically offer browser extensions for added safety on sites that take passwords or other secret information. Such extensions are generally free of charge, but must be installed to be effective.

NEVER buy or download an alleged security program or browser extension in response to an unexpected pop-up advertisement or email message. Such messages often claim that your computer has been scanned and found to have security problems. The "programs" they offer are usually frauds that would put rogue software on your computer.

Account Authentication Measures

To protect your accounts at Internet sites, online services, and other ways you do business remotely, you need strong passwords. The suggestions below will help you create them.[3] Password strength is most important for sites that keep your money or personal information.

(1) Make each password at least 8-10 characters long. Long passwords *usually* are better than short ones. But "password1234" (for example) is very weak even with 12 characters, because password-guessing software, described below, would try it quickly.

(2) Do not include in a password anything that someone else might guess would be in it. That includes all parts of your name and address (including city or state); significant dates; the name of a sports team, music group, celebrity, or business; and anything else that is guessable. The more obscure something is, the better it is in a password.

(3) To make a password that you can remember, try one of these methods:

   (a) Think up a sentence that forms a memorable mental picture, and make a password from the first letter of each word in it and each number or other character in it. "We saw 3 kangaroos & 7 peacocks @ the zoo on Friday" would make this strong password: Ws3k&7p@tzoF

   (b) Combine a few full words that no one would guess, plus numerals and other symbols, in a password. For example: Kale8Rocks#Boat5

(4) Do not use the same password for more than one important account. If hackers learn it, the other accounts will be vulnerable.

Guessable elements make passwords much less secure. If hackers break into a site that holds your password—even in encrypted form—and it has guessable combinations of characters, the hackers may be able to "break" it using password-guessing software. The details are a bit technical; but such software is used to try many common words and combinations quickly until a match is found to information about the password stored on the site (called a "password hash")—revealing that the combination is your password. Computer security researchers have found that the same or very similar passwords are commonly chosen by many users.[4] Password-guessing software would start with obvious ones.

Many people use "password manager" software to store their passwords, using a main password to unlock all their passwords to online sites. That is safer than writing passwords on paper—or worse, storing them in an unencrypted computer file. There is at least a slight risk that hackers may someday defeat the security of the password manager and steal your passwords—particularly if they are stored online, as they commonly are. The decision whether to use a password manager involves balancing the risks of such a security breach against the risk of theft of a password stored in a way that may be less secure.

Another valuable safeguard for financial and other sensitive accounts is two-factor (or multi-factor) authentication. This involves something, in addition to typing your password, that you must do to enter your account—often typing a multi-digit number that the company sends you by text or voice message. This greatly reduces the risk that unauthorized persons will enter your account.

Care in Clicking

Clicking on links and buttons on a computer, phone, or other Internet-connected device, without knowing where they lead, risks downloading harmful software. The more devices you have connected to the Internet, the greater your risk. If they are connected through services such as iCloud or Google, scammers may be able to enter several devices easily.

To avoid downloading malicious software:

- Ignore clickbait (eye-catching links to unknown sites).

- Do not investigate offers on social media—or anywhere else—that seem too good to be true.

- Do not open attachments from people you don't know. Even if you do know the apparent sender, be very careful about opening an attachment. A hacker may have taken over the person's email account and sent messages with rogue attachments; or the person may have forwarded the attachment to you without knowing that it carries malware.[5]

Common kinds of scams

Scammers constantly think up new ways to trick people into sending money or personal information. But there are common threads in many scams that should put you on guard.

Telephone Scams

Scams by telephone, including text messages, often try to create fear by warning that something bad is about to happen. They may claim that there is a "problem" or "suspicious activity" with your Social Security number, or bank or credit card account, and tell you to contact them to resolve it. Or they may warn that you owe a tax or fine and will be arrested unless you pay it immediately. You should hang up on or delete all such messages. (If you worry that such a message may be valid, call or email the agency or company that allegedly sent it, using contact information from its website or the phone book—NOT from the message, which would send you to the scammer.)

It is a huge red flag if a caller tells you to pay by buying a gift card and sending numbers from it. Government agencies and legal businesses do not ask to be paid by gift card—but scammers do, since it is difficult or impossible for such funds to be tracked.

A caller may even claim that one of your relatives (such as a child or grandchild) has been arrested or is in trouble, and demand money for bail, medical care, etc. This scam seeks to get you to act without thinking first. If the caller won't let you speak with that relative, no more evidence is needed to show that the call is a fraud. But you should report it to police so they can warn the public of the scam.

Email scams

Scam email messages, like phone scams, may try to create fear, such as by claiming that your email account has been compromised. But many email scams target people's desires. They may claim that:

. . . you have won a valuable prize (even though you didn't enter a contest).

. . . their product can solve problems that you may—or may not—have, or make your computer work better.

. . . romance is only a click away.

Email service providers keep adjusting their "spam filters" to catch such messages; scammers keep using new ways to trick people into opening them. If you get a message like those described above, that did not go to your spam folder, mark it as spam to help your provider catch such messages, and delete it without opening it. (If you open it, the sender may get a "received" message and send you more spam.)

Opening a fraudulent email message has bigger risks than merely getting more such messages. At the least, you may buy something but not get it. Worse, criminals may use your payment information to put charges on your credit card or bank account, and information that you send may make you a victim of identity theft. Perhaps worst of all, clicking a link in a fraudulent message can enable criminals to put malware on your computer, as described below. You may then face financial (and perhaps legal) harm from the malware.

If you have already sent personal information to what you now think was a scammer, visit IdentityTheft.gov for ways to protect your identity.

Phishing

Phishing seeks to trick you into revealing personal or financial information—usually using fraudulent email messages or websites. The sender is "phishing" (fishing) for your information for criminal purposes. Unlike other scam email, phishing messages may be tailored to you, using facts about you from social media or other public sources.

Phishing messages may resemble official notices from a trusted source such as a bank, credit card company, or other firm where you do business. They may claim that there is a problem with your account, and ask you to click on a link to log in with your username and password. But the link would actually take you to a fraudulent website that would steal your information.

Do not reply directly to messages asking for personal or financial information. **Do not** click on links in them—even if they seem to be from organizations you trust. Legitimate businesses do not ask you to send sensitive information using insecure channels such as email. If in doubt, contact the alleged sender by logging in to its site using a bookmark, or carefully typing its Internet address into your browser, and report the message you received.[6]

Illinois' Anti-Phishing Act prohibits using the Internet to try to get identifying information from anyone by claiming to be a business, without the consent of that business.[7] But phishing messages may come from overseas and be difficult or impossible to prosecute under state or federal laws.

Malware

Malware (malicious software) is any software that does things you do not want, usually to benefit its sender. Categories of malware include viruses, worms, Trojan horses, and spyware. Effects of malware can include serious computer damage and theft of sensitive information such as passwords, if they are stored in your computer. It may cause your computer to crash or become inoperable, or be used to spy on your online activity.

A particularly harmful kind of malware is ransomware. If it gets into your computer, it will encrypt all of your files, making them useless to you—unless you pay a ransom to the hackers, who usually are overseas. They will demand payment in a cryptocurrency to prevent it from being tracked to them. Even if you pay, there is no guarantee that they will send you a software key to unlock your files. To guard against ransomware, make backups of all important files, and update them when you change or make new files.

Computer security practices such as those mentioned earlier can help you avoid malware. Use security software and keep it updated. Do not click on links or open attachments in messages that are unsolicited or from unknown sources. Use browser security settings to detect and prevent unauthorized downloads. Use a pop-up blocker, and don't click on links in pop-up advertisements. Don't download software in response to unexpected pop-

up or email messages—especially if they claim to report problems in your computer. Download software only from known and trusted websites.

Even following all those rules cannot make you completely safe from getting malware on your computer. So you should have a backup routine for all important files and other data. If they are encrypted or erased—or the computer becomes unusable and must have its data wiped clean—your important files will still be available.[8]

"Technical Support" Scams

Technical support scams exploit computer users' concern about malware and other threats. Scammers call or email and pretend to be technicians for a well-known (or real-sounding) software company, and say there are viruses or other malware on users' computers. They want to trick users into granting them remote access to their computers, and/or buying software of doubtful value.

A simple rule will guard against these scams: If any source, other than your own computer security software, claims to have found a problem with your computer, hang up or delete the message. If you think it may be true, do a complete scan of your computer using your computer security software. Also, never disclose a password by phone, or give someone whose identity you are not sure of remote access to your computer.[9]

Spam

The word "spam" (not capitalized) describes commercial email distributed widely without recipients' consent. If you delete it without opening it, it is only an annoyance. But much spam comes from cybercriminals seeking to steal money or personal information, and/or load malware on victims' computers.

Email providers use spam filters to block suspected spam, or to send it to a "junk" or "spam" folder. Marking obvious spam messages as junk or spam will help your email provider catch similar future messages.

Another way to limit spam is keeping your email address as private as possible. Try not to put it in blog posts, chat rooms, social media sites, or online membership directories, which spammers may use to get addresses. If a site with which you need to do business requires an email address, consider giving an alternative address that you have created for such purposes. The reason is that many businesses, and some nonprofit organizations, sell users' email addresses to others. Any address that you give to a business may begin getting spam—at least unless the business emphatically promises not to sell, rent, or otherwise transfer your information to another entity. But you will need to check your alternative address periodically for any important messages from businesses to which you gave it.

As with your primary email address, an alternative one needs a strong password, so hackers cannot take it over and block you from receiving messages—which could inform you that someone has changed your password for that business, or begun withdrawing money from your account.[10]

Delivery of ordered items

A Federal Trade Commission regulation says that a company selling by mail, telephone, or online must ship the goods within its advertised time period—or, if it does not advertise one, within 30 days after it receives the order (50 days if you applied for credit on the order). If shipment cannot be made by then, the company must give notice and an option to cancel and get a refund. The seller can seek your consent for possible future delays; but if you consent, you have a right to cancel for a refund at any time before shipping. The seller also can cancel and refund your money if it cannot ship within the original time, or a longer period to which you consented. The 30-day rule does not apply to magazine subscriptions after the first issue arrives; seeds and growing plants; or COD orders.[11]

If something you ordered does not arrive in 30 days (unless the advertising said it would take longer), inform your local post office; visit https://reportfraud.ftc.gov/#/; or call the FTC Help Line at (877) 382-4357.

Protecting Your Money, Credit, and Identity

Even if you never buy online or use a mobile app, your choices for payments and payment methods can have major effects on your financial health. This section discusses options for keeping what you have earned.

Credit and debit cards

How can I find the best credit card deal?

Comparing card issuers is wiser than answering an online or mailed offer. Some finance websites list what they consider to be the best credit cards, often classified by type of card user. Things to look for when deciding where to apply include:

Photo by: Reza Luke via Wikimedia

- What interest rate(s) will you be charged if you do not pay in full by each due date? (Only a minority of card users pay in full every month. But if you are confident that you will, the interest rate may be less important.)

- If you are ever late in paying, will the issuer raise your interest rate? (Issuers typically do, because late payment may be a sign of higher credit risk.)

- How much protection does the issuer promise against liability for unauthorized charges? As discussed later, there are legal limits on your liability if you report a lost or stolen card and can show that you did not make or authorize a charge. Some card issuers say that you will not have to pay any unauthorized charge if you gave prompt notice.

Think twice before applying for a card simply because it offers 0% interest for several months. The issuer is betting that you

will start paying interest after that—at a rate that may be higher than you could have found elsewhere.

Is it better to buy using a credit or debit card?

Each has pros and cons. A credit card lets you buy things that you can't pay for immediately. But that convenience has a high price in interest charges unless you pay all you owe by the due date. Using a debit card, check, or cash can help in controlling spending. (Many banks offer overdraft protection for checking accounts, but at interest rates similar to those for credit cards.) Debit cards may be somewhat less safe against unauthorized charges than credit cards. Each kind of card has some risk of fraudulent use.

How can I protect against fraudulent charges?

Keeping your cards safe is the first step. When you use a card, it should stay in sight until it is back in your wallet or purse. Unscrupulous employees at some businesses may copy numbers from cards and use them for fraudulent purchases, or sell them to others who will.

Many credit card issuers have monitoring programs to detect unexpected patterns of use. After unusual charges, they may freeze your account until you confirm the charges. You may want to call your card issuer(s) before a major trip—especially overseas—to reduce the chance that this will happen. Some issuers also let you opt to receive email or text alerts of suspicious charges.

See "*What if my card is lost or stolen?*" below for more information.

What if my credit card statement shows charges I didn't make?

Notify the issuer by phone or online, and confirm with a letter as soon as you can. The letter must give your name and account number; describe what you think is wrong; and explain why. You should enclose copies of any documents supporting your claim, such as receipts for returned merchandise. Mail it to the address on your bill under words such as "Send inquiries to:". The issuer must acknowledge the letter within 30 days. Within

90 days after getting the letter, it must either adjust the bill or explain why it believes the bill is correct. Until then, you need not pay charges that you dispute. But the issuer can calculate interest, and apply the amount that you dispute against your credit limit.[12]

You should keep all credit and debit card receipts (including ATM receipts) and compare your statements to them. (Statements and receipts should later be shredded or kept in secure storage.)

What if my card is lost or stolen?

Call the issuer at once. Within hours (or even sooner), a thief may use up a credit card's credit limit or a bank's daily limit on withdrawals through a debit-ATM card. Thus, you should be prepared to call the card's issuer quickly. Make a list containing each phone number you will need, and keep copies separate from your cards. If any are lost or stolen, call the issuers, then confirm in writing.

For a credit card, you should not be liable for more than $50 of unauthorized use *before* you notify the issuer, or for any amount of unauthorized use *after* you notify it.[13]

For a debit-ATM card, if you report loss or theft to the issuer within 2 business days after learning of it, your liability for fraudulent charges made *before* you reported is limited to $50. You may be liable for up to $500 of charges made *more than 2 business days after* you learned of its loss or theft and before you reported it. You should have no liability for fraudulent charges made after you reported.[14]

To benefit from these legal protections, you may need to show the card issuer (and perhaps even a court) that charges or withdrawals were unauthorized. Thus, it is better if you notify the issuer before someone who stole your card, or found it after it was lost, can use it.

What is the law on denying credit-card applications?

No person who properly applies may be denied a credit card due to race, color, religion, national origin, ancestry, age between 40 and 70, sex, marital status, physical or mental handicap not related to ability to pay, or unfavorable military discharge.[15] A card

can be denied for failure to meet the issuer's objective standards of creditworthiness. These usually include income, other current debts, and record of repaying debts.

Credit histories and scores

Consumer reporting agencies (also known as CRAs or credit reporting agencies) collect consumer credit information, evaluate it, and distribute reports on it to their customers, including lenders.[16] The U.S. has three major CRAs: Equifax, Experian, and TransUnion. Others, including Innovis, collect credit information for limited purposes, such as employee or tenant screening or making pre-approved card offers. If you have, or in recent years had, any loans or accounts involving credit, those companies very likely have information on you.

What information does a CRA gather and report?

Files kept by a CRA generally have a person's name, age, Social Security number, and places of residence and employment; financial information such as income, bank accounts, home values, and debts; and character or reputation information, such as any lawsuits, arrests, and convictions.

Such information makes up the person's "credit history," which lenders, landlords, and some other businesses use to help them evaluate applicants for things such as credit, housing, or insurance. So it is important to establish and keep a good credit history by using your credit responsibly.

Can employers use my credit history in hiring decisions?

Under Illinois law, an employer may not obtain or use a report on an applicant's credit history for employment purposes unless having a satisfactory credit history is a *bona fide* occupational requirement for the work. A satisfactory credit history is such a requirement if either (1) or (2) below is true:

(1) The position involves:

- custody or unsupervised access to cash or assets worth at least $2,500;

- signatory power over business assets of at least $100 per transaction; or

- access to personal, confidential, financial, trade secret, or state or national security information.

(2) Any of the following is true:

- The position is managerial and involves directing or controlling a business.

- State or federal law requires a bond or other security for a person holding such a position.

- A U.S. or Illinois Department of Labor regulation lists that kind of position as one for which a good credit history is a *bona fide* occupational requirement.

- Credit history use is otherwise required by federal or state law.[17]

What is a credit score?

A credit score is a three-digit number used as a quick gauge of how reliable a person will be as a borrower. Many businesses pay credit reporting agencies for credit scores on would-be customers. Major banks and other lenders may calculate credit scores for use in their lending. Thus, one person may have several, somewhat different, credit scores. Some companies offer to tell you their credit scores on you, usually in return for something of value to them.

It is worth the effort to earn, and keep, a good credit score to get lower interest on loans; higher credit limits; and other opportunities not offered to people with low credit scores.

How can I raise my credit score?

"Credit repair" businesses claim that they can raise your credit score for a fee. Although they are not necessarily fraudulent, they offer services that you could do for yourself: Checking your credit files and challenging anything you consider inaccurate that tends to lower your score (as described below). The most effective way to improve poor credit is to make all payments on time. Reducing your balances on "revolving" loans, such as credit card debt, can also help raise your score.

Can I see the information in my credit file?

At your request, with proper identification[18] and payment of a "reasonable" fee (unless an exception applies), a consumer reporting agency (CRA) must disclose to you all information in its file on you, other than credit scores or ratings.[19] You can also ask for a CRA's credit score on you, but it can charge a separate fee for it.[20] On request, the CRA must also tell you about anyone who received a report on you for (a) employment purposes in the last 2 years or (b) any other purpose in the last year.[21]

A nationwide CRA must provide one free credit report per year upon request.[22] (Visit www.annualcreditreport.com to make a request.) A report that you request within 60 days after being notified that your credit rating may be adversely affected by a report, or that an action unfavorable to you has been taken based on a credit report, must also be free of charge.[23]

What should I do if my credit file has incorrect information?

Inform the CRA. It must reinvestigate and delete any information that is false or cannot be verified. If reinvestigation does not resolve the matter, you can put an explanation of the dispute in your file. Any credit reports issued later that contain the disputed information must note that it is disputed, and include either your statement or a clear and accurate summary of it. You can require the CRA to send that statement or summary to a prospective employer that received the disputed information in the last 2 years, or to any other entity that received it in the last 6 months.[24] The CRA can charge you a "reasonable" fee to do so—unless you make the request within 30 days after being told that your credit rating has been, or will be, adversely affected by the report.[25]

To dispute credit information, contact one or more of the following:

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
Two Baldwin Place
1510 Chester Pike
Crum Lynne, PA 19022
(800) 888-4213
www.transunion.com

Innovis
P.O. Box 530088
Atlanta, GA
30353-0088
(800) 540-2505
www.innovis.com

The following section has information on contacting these companies if you suffer fraud, or want to "freeze" your credit information.

Identity theft

What is identity theft? What should I do if it happens to me?

Identity theft is unauthorized use of your personal information—such as your name combined with your birthdate, Social Security number, and/or account number(s)—to commit fraud or theft. Identity thieves may set up credit card, bank, or other accounts in your name, or change the mailing address on your accounts and use them without your knowledge.

Signs of identity theft can include failing to receive expected bills or other mail; receiving credit cards (not mere applications for them) that you did not request; being denied credit for no obvious reason; and being contacted by debt collectors about money you did not borrow.

If you suspect that you are a victim of identity theft, call the Illinois Attorney General's Identity Theft Hotline at (866) 999-5630 (TTY (877) 844-5461). It has several resources, including trained advocates to help you take these steps:[26]

1. Contact any creditors involved to report the fraud, and to check whether any new accounts have been opened in your name or further unauthorized charges have been made. Close fraudulent accounts. If you open any new accounts, select completely new Personal Identification Numbers (PINs) and passwords for them.

2. Put a fraud alert on your credit report and get a free copy of the report (as described in the preceding section). A CRA that you contact is required to notify the other two major CRAs of a fraud alert.[27]

3. File a report with your local police. Illinois law requires police departments to accept and provide copies of identity theft reports.[28] Get a copy of the report and keep it in case your bank, credit card company, or other financial services provider asks for it.

4. Consider putting a freeze on your credit reports. A freeze prevents release of your reports to lenders without your consent, to prevent criminals from borrowing in your name. (If you ever need to apply for new credit, you can temporarily—or permanently—thaw your credit for that lender, using a passcode known only to you and the CRA.) A CRA may not charge Illinois residents to freeze or thaw their reports.[29] To make a freeze fully effective, you must request it from all three major CRAs:

   Equifax

   www.equifax.com/personal/credit-report-services/credit-freeze/

   Experian

   www.experian.com/freeze/center.html

   TransUnion

   www.transunion.com/credit-freeze

5. Keep informed by requesting a copy of your credit report

from one CRA every 4 months (once a year per CRA). You can get these reports at:

www.annualcreditreport.com

or by calling (877) 322-8228.

How can I prevent identity theft?

The Illinois Attorney General and other sources recommend methods such as these to guard against identity theft:[30]

- When choosing passwords or PINs, avoid using anything that identity thieves could find online (such as your mother's maiden name, or your or a family member's birthdate) or could guess (such as the name of a sports team, celebrity, or other popular term).

- Do not provide any personal information (including a birthdate), or information on financial or other accounts, by phone, mail, or online unless you are certain of the recipient's identity. A good (but not perfect) way to know who you are dealing with is to contact the entity that seeks the information, at a phone number or Internet address that you know belongs to that person or institution, to give the information. Never send confidential information in an unencrypted email message—it is not secure.

(See also the discussion of computer security on pages 1- 4 of this booklet.)

- Put outgoing mail only in an official collection box (preferably indoors) or a post office, and retrieve mail from your mailbox promptly. Before traveling, visit www.usps.com or call (800) 275-8777 to request a vacation hold on your mail.

- Shred any trash containing personal information.

- Do not carry your Social Security card. If you have a choice, use identifying information other than your Social Security number, such as a driver's license or state ID card number.

- Ask your employer, and businesses or institutions that collect your personal information, about their information security measures. If many people raise the issue, organizations will take notice.

Safety for Minors

Online sites, such as chat rooms and social media sites, and text messages can expose minors to material and conduct not appropriate for them. Worse, electronic predators can threaten their privacy and safety. The anonymity of many electronic messages makes it easy for criminals to misrepresent themselves and manipulate or trick users who are accustomed to trusting people. Even adults can fall victim to such ploys; minors tend to be easier targets. Cyberbullying is also a growing problem.[31]

How can minors avoid becoming victims?

Minors can do several things to stay safe using electronic communications:[32]

- Never give out personal information, such as address, phone number, or school's name or location, without a parent's permission.

- Choose a screen name that does not reveal personal information—including your name.

- Do not send pictures of yourself to anyone without parental permission. Sending intimate pictures ("sexting") is particularly dangerous because it can lead to blackmail—or worse.

- Do not agree to meet an online "friend" alone—especially in a place that is private or dark, or where there are few people. Any meeting with someone you do not already know in person should be in a well-lit, public place, with at least one parent or other responsible adult present.

- If something online makes you uncomfortable or uneasy, tell a parent. Do not reply to any message that makes you uncomfortable.

- Follow family rules on computer and phone activities.

- Remember that people online may not be who they claim to be.

What can adults do to protect minors from these dangers?

Parents and other adults with responsibility for minors (such as teachers) can take active roles in supervising their online activities in ways such as these:[33]

- Discuss with them how electronic interaction—including text messaging, emailing, and downloading files or software—has dangers not present when interacting in person. Make sure they understand that **no one** regulates what is available online. The fact that something is online does NOT mean that it is safe, truthful, or wholesome.

- Be aware of Internet sites that children in your care visit. Consider using blocking or screening services for them, available through Internet providers, browsers, and companies specializing in such protection.

- Set up an account for each child in any computer the child is allowed to use, with a different password for that child. (All accounts should have strong passwords; see page 3 of this booklet.)

- Create and enforce rules on computer use.

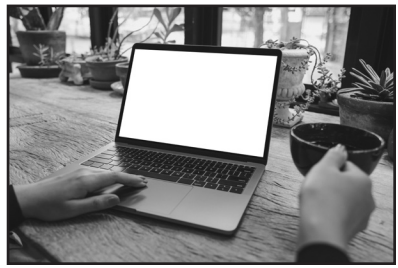
- If practical, keep any computer to which children have access in a room other than a child's room, with people frequently passing by, so times of use and material viewed can be monitored.

- Learn the functions and capabilities of software used by each child.

- Ask about people your children meet online. Discuss online experiences just as you would ask them about a day at school.

- Spend time with your children when they are online. Observe their online practices firsthand. Set a good example for children with your online habits.

Laws on Minors and Internet Safety



Federal and Illinois laws seek to promote Internet safety and protect minors' privacy. The first two laws listed below are federal.

The Children's Online Privacy Protection Act of 1998 regulates sites' collection of personal information from anyone under 13. It imposes requirements on online providers of services for children, and other site operators having knowledge that they have collected information from children. Such companies must provide notice of their privacy policies; obtain verifiable parental consent before collecting personal information from children; allow parents to examine and delete personal information provided by their children; and create and follow reasonable procedures to protect the security of personal information received from children.[34]

The Children's Internet Protection Act allows schools and libraries to get discounts on Internet service, provided by federal law, only if they use filtering technology and other measures to protect children from harmful content.[35]

Illinois' Online Child Safety Act requires each Internet service provider to offer parental controls allowing parents to do at least one of the following (chosen by the provider):

(1) List specific sites, or categories of sites, that their children may <u>not</u> visit.

(2) Limit the sites, or categories of sites, that their children <u>may</u> visit to those on an approved list.[36]

The School Code provides for annual, age-appropriate Internet safety instruction in grades 3-12.[37]

Installment sales; collection agencies; repossession

Buying on an Installment Plan

An alternative to using a credit card, or otherwise borrowing from a financial institution when buying things such as vehicles or appliances, is an installment sale, in which the buyer promises to make weekly or monthly payments until the entire cost is paid. Illinois' Retail Installment Sales Act[38] and Motor Vehicle Retail Installment Sales Act[39] regulate those sales. An installment sales contract must be signed and dated by both parties, and show the number of payments; their total amount; itemized charges; and other important information.[40] Amounts to be paid may include interest, fees, and taxes in addition to the price.[41]

If the buyer fails to make required payments on time, the seller (or a finance company that bought the contract from the seller) may "repossess" the item.[42] The Retail Installment Sales Act provides some protections to a buyer of an item, except an automobile, who had paid a significant part (30% or 60%) of the total amount owed before repossession occurred.[43] However, this way of buying is likely to cost more than using a credit card, if the card's interest rate is reasonable.

Collection Agencies

Lenders can legally hire collection agencies to collect amounts owed to them. Illinois laws put restrictions on such agencies' activities, as described below.

May a collection agency call me 24 hours a day?

No. A collection agency can be disciplined under Illinois' Collection Agency Act for calling you or your family at home between 9 p.m. and 8 a.m. without permission from you or a court; or for repeatedly or continually calling you with intent to annoy, abuse, or harass you.[44]

What other acts by an agency are prohibited?

The list of collection actions for which a collection agency can be disciplined includes:

- Threatening violence to you or your family or property.[45]

- Threatening to seize your property that by law can be taken only with a court order—unless the collector discloses that court proceedings are necessary before taking it.[46]

- Releasing or threatening to release false information to harm your credit reputation.[47]

- Using profane, obscene, or abusive words in communicating with you or your family.[48]

- Disclosing or threatening to disclose information about a debt to persons who have no legitimate business need for it, unless the disclosure is regulated by law.[49]

May I refuse to communicate with a collection agency?

Yes. You can notify a collection agency in writing that you want to cease communication with it.[50] After receiving such written notice, the collection agency cannot communicate with you except to notify you of any of the following:[51]

- That the agency's efforts to collect the debt have ended.

- That the agency may invoke specified remedies (such as a lawsuit) ordinarily used by such a collection agency.

- That the agency intends to invoke a specified remedy.

How much time do I have to dispute a reported debt?

Within 5 days after first communicating with you to collect a debt, a collection agency is to tell you that if you do not dispute it within 30 days after getting notice of it, the collection agency will assume that it is valid. (But the Act adds that your failure to dispute a reported debt within those 30 days does not constitute an admission of liability for it.) If you do dispute the debt, the collector must stop trying to collect until it is able to verify the debt and mail that information to you.[52]

Buying a Vehicle

Comparing quality and features

The U.S. Department of Transportation's National Highway Traffic Safety Administration (NHTSA) offers a 5-Star Safety Ratings Program, which provides information on crash protection and rollover safety of new vehicles. Some other organizations test vehicle safety. But NHTSA says that only it rates resistance to rollover in addition to front and side crash injury.

NHTSA recommends that drivers seek vehicles with these driver assistance technologies that meet NHTSA performance tests:[53]

- Forward collision warning
- Lane departure warning
- Automatic emergency braking
- Rearview video system

NHTSA's vehicle safety ratings are posted at:

www.nhtsa.gov/ratings

Several websites allow consumers to compare vehicle features at no charge. The most popular include:

Kelley Blue Book
www.kbb.com/compare-cars

J.D. Power
www.jdpower.com/cars/compare-cars

Edmunds
www.edmunds.com/car-comparisons

Efficiency ratings

Each new car has a label giving information on its fuel economy. The U.S. Environmental Protection Agency (EPA) gives each vehicle a rating of 1 (worst) to 10 (best) on two measures:

(1) Fuel economy. For vehicles using liquid fuel, such as gasoline, this number is miles per gallon of fuel (MPG). If a vehicle does not use liquid fuel, the EPA calculates the number of miles it can go on an amount of fuel that has the same energy content as a gallon of gasoline, to enable comparisons between vehicles using different fuels. This is called "miles per gallon of gasoline equivalent" (MPGe).

(2) Greenhouse gas emissions. This is how much carbon dioxide the vehicle emits per mile.

Most vehicles have only one rating, because carbon dioxide emissions are directly related to fuel use. A gasoline-powered vehicle has the same rating for fuel economy and for greenhouse gas emissions. If a vehicle's fuel economy and greenhouse gas emission ratings differ, its label shows both ratings. [54]

Vehicles' fuel economy numbers are posted by the U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy at:

www.fueleconomy.gov/feg/findacar.shtml

Buying on credit

The two main ways to borrow money to buy a car are direct lending and dealership financing.

Direct lending is borrowing from a bank or other lender, such as a credit union, that is not connected with the dealer. This allows the buyer to learn credit terms and comparison shop among dealers. Dealership financing is done through the dealership selling the vehicle. It may involve a variety of financing options due to the dealer's relationships with multiple lenders; dealers also can sometimes offer special incentive programs.

It is best to compare financing offers from several lenders and one or more dealers. The Federal Trade Commission (FTC) cautions not to look only at the amount to be paid per month. Many lenders offer long-term loans with low *monthly* payments but high *total* costs because they take more years to pay off. The FTC also recommends negotiating the annual percentage rate (APR) with the dealer. The APR is the cost of credit on an annual basis. The APR offered to each buyer depends on several things, including the buyer's credit rating; the amount to be borrowed; market interest rates and credit costs; and the length of the loan. It usually includes an amount to compensate the dealer for handling financing.

Some dealers and lenders may ask buyers to buy credit insurance to pay off their debt if they die or are disabled. Credit insurance is not required by federal law. Including it in a loan without the buyer's knowledge is illegal.[55]

If a vehicle is financed, the lender gets a lien on it until the loan is fully paid. That means that if the buyer misses payments, the lender can repossess the vehicle. Late or missed payments can have other serious consequences, including making future credit harder to get.[56]

Extended warranties

Illinois' Service Contract Act regulates contracts in which a company promises, over a stated time and for a stated amount, to pay for repairs on a car or other consumer product. Such a contract must clearly state its terms, which must include an option to cancel. If the buyer cancels, the company can keep a cancellation fee of up to 10% of the contract price or $50 (whichever is less). If a contract is cancelled within 30 days after the purchase and no repair service was provided, the buyer can get a full refund minus a cancellation fee. If it is cancelled later, the buyer is to receive a pro-rated refund minus the value of any service provided.[57]

Getting defects repaired: new cars

Illinois has a "lemon law" for buyers of new cars (and persons leasing them for at least 1 year) that have excessive defects in the first 12 months or 12,000 miles, whichever comes first.[58] If you have problems with a new car or light truck, you must first try to get it repaired under its warranty by an authorized dealer for the manufacturer. The law states a presumption that a "reasonable number of attempts" at repair has been made if:

(1) the authorized dealer(s) have been unsuccessful at repairing the problem after at least four attempts during the warranty period; or

(2) the vehicle has been out of service for repairs for at least 30 business days during the warranty period.[59]

If either of those is true, and the dealer is still unable to make the vehicle perform as warranted, you must then try any "informal settlement procedure" that the manufacturer has provided (and of which the dealer has given you written notice).[60] Even if there is no such procedure, you must send written notice directly to the manufacturer and give it a chance to correct the problem.[61] If neither the dealer nor the manufacturer can correct the problem after a "reasonable number of attempts" as described above, the law says you are entitled to either a new vehicle or a refund (minus an allowance for your use of the vehicle you had).[62] Any suit for a refund must be filed within 18 months after first delivery

of the vehicle to you[63]—but times during which your dispute is "pending" under an informal settlement procedure do not count toward those 18 months.[64]

Getting defects repaired: used cars

If you buy, from a licensed vehicle dealer or at a public auction, a used motor vehicle with no more than 150,000 miles on it and a weight rating not over 8,000 pounds, the dealer must pay part of the cost of any repairs to a powertrain component that are needed within 15 days after you receive it or until you drive it 500 miles, whichever is earlier—except repairs needed due to abuse, neglect, failure to do regular maintenance or maintain required fluids or lubricants, off-road use, racing, or towing. Days when the vehicle is nonfunctional are excluded when calculating the 15-day period. This law does not apply to vehicles with certificates of title labeled "rebuilt" or "flood," or to antique or collector vehicles.

Powertrain components include the engine block, head, all internal engine parts, oil pan and gaskets, water pump, intake manifold, transmission, torque converter, drive shaft, universal joints, rear axle, and rear wheel bearings. You must pay half the cost of the first two repairs needed to make the vehicle functional, up to a maximum of $100 per repair (or a total of $100 if the second repair is for the same defect as the first one).[65]

Buying a Home

Buying a home can be exciting. It can also be stressful. Homebuyers must make many decisions—often quickly and with limited information. This section addresses some major steps in the process. You may also want to seek guidance from family or friends; a book on homebuying; and/or an experienced real estate agent.

Buyers should do a few things *before* they start house hunting. Those include:

- Deciding what kind of mortgage to apply for.

- Comparing interest rates and other details of loans.
- Applying for pre-approval for a mortgage.

Types of mortgages

A mortgage is a long-term loan (usually for 15 to 30 years) in which real estate is used as security to the lender for repayment. (This topic is discussed under "Effects of default" below.) Since the repayment period is so long, how you pay interest can have a major effect on your total borrowing costs. Mortgages fall into two classes based on how their interest is calculated:

A *fixed-rate* mortgage has the same interest rate, and equal monthly payments, throughout its life. For example, if a 30-year, fixed-rate mortgage has an initial monthly payment of $750, the borrower is to pay a total of $270,000 over 30 years ($750 x 12 x 30).

An *adjustable-rate* mortgage's interest rate, and monthly payments, change periodically (typically each year) based on an index of market interest rates. There may also be a minimum and maximum rate payable, regardless of how high or low market rates go.

Fixed-rate mortgages may seem simpler than adjustable-rate ones, but the reality is more complex. No one can predict inflation or interest rates for 30 years. If inflation rates are low during the term of a fixed-rate mortgage, it will end up costing a substantial amount in "real" dollars (dollars adjusted for inflation), because the dollars used to pay it off will not be worth much less than those that were borrowed. By contrast, if there is high inflation during the mortgage term, borrowers will pay with dollars worth much less than those they borrowed. Another fact is that if market interest rates fall significantly from their levels when a fixed-rate mortgage was made, borrowers can save money by "refinancing"—getting a new mortgage at a lower rate in lieu of the initial mortgage, although that involves fees and other costs.

Because fixed-rate borrowers may be able to repay with dollars worth much less after inflation, or to refinance at lower rates, a fixed-rate loan's interest rate tends to be higher than the initial rate on an adjustable-rate loan made at the same time. A higher fixed rate compensates the lender for taking two risks: The risk of being repaid in dollars worth much less, or of being repaid early and having to re-lend the money at lower rates.

For these reasons, neither type of mortgage is best for all borrowers. In general, adjustable-rate mortgages may be better for persons buying homes early in their careers, whose incomes are likely to rise considerably during their terms; fixed-rate mortgages may be better for persons buying later in life, and/or whose incomes are unlikely to rise much—especially if they will retire before paying off the mortgages. You may want to use financial software to project possible scenarios for inflation and interest rates before choosing what kind of mortgage to seek.

Comparing interest rates

Along with choosing a mortgage type, would-be homebuyers should look at rates offered by local and national lenders, because one lender's rates may fit them better than rates of other lenders. That can be particularly true of adjustable-rate mortgages, because they are structured in various ways. Many start with a low introductory rate that will rise at a stated time. Other ways in which such loans differ are what "index" of interest rates will be used in adjusting the rate; how often the rate will be adjusted for changes in that index; and whether the rates to be paid are subject to minimum and maximum levels. All these things should be taken into account when comparing lenders.

Would-be homebuyers should also think about their credit scores (discussed under "Credit histories and scores" on pages 13-14). It's a good idea to learn the credit score of each person who will be obligated on the mortgage. A lender, such as a credit card issuer, may be willing to provide that information. If at least one person who will be liable on the mortgage has a low or borderline credit score, the suggestions in that section of this booklet may be helpful for raising it.

Applying for pre-approval

It is important to apply for mortgage pre-approval before you try to buy, because you need to be able to act quickly if you find a place you want. With pre-approval, you can make an offer to the seller—usually accompanied by "earnest money" from your savings (not from the lender) to encourage the seller to consider your offer. Pre-approval lets you do that without risking loss of the earnest money (it will not normally be returned if you sign a purchase contract but are unable to buy the property).

Mortgages are offered by banks; many credit unions; and mortgage companies (regulated separately from banks and credit unions[66]). To apply for mortgage pre-approval, you may need documents showing your financial status—especially assets and income, which a credit report does not normally show. Some lenders may charge a fee for considering your application.

Effects of default

If you stop making payments on a mortgage before it is paid off, the lender can foreclose—taking the property and selling it to collect the unpaid balance, plus fees and expenses. If that happens, you will normally receive any sale proceeds left after paying those amounts.

Illinois law has protections for mortgage borrowers who get behind on payments. The main protection is the ability to "redeem" the property (reversing the foreclosure) for some time after notice of foreclosure, by paying the amount due plus costs. For residential property, that time is usually 7 months.[67] But a homeowner seeking to redeem must notify the lender's attorney at least 15 working days (3 weeks or more) before that time ends.[68] Also, an owner ordinarily cannot redeem a property more than once every 5 years.[69]

Buying by "contract for deed"

Another way to buy a home on credit is called "contract for deed," in which the buyer contracts to pay the seller—not a mortgage lender—periodically over a number of years, for the price

plus interest. While making such payments, the buyer gets to live in the residence. If the entire debt is paid off, the buyer gets a deed to it.

This financing method has typically been used by buyers who could not get mortgages due to weak credit histories. It gave buyers less protection than a mortgage did; buyers who got behind in making payments could lose all they had paid (except the rental value of living in the residence up to that time). A 2017 Illinois law provided more protection to buyers who use this method.[70] This law applies to any person or business that sells four or more pieces of nonfarm, residential real estate (each having one to four dwelling units) by this method within 12 months.[71] Such a seller must comply with many requirements, including giving detailed information on the loan terms in the sales contract;[72] having the contract recorded in the county recorder's office;[73] and allowing a buyer who gets behind in making payments 90 days to remedy the default by paying all charges then due.[74] For 3 business days after accepting an "unexecuted" contract for deed with such a seller, the buyer has a right to cancel and get back any money already paid.[75]

For More Help

If you have a problem with a business, first contact it and ask it to resolve the problem. Reputable businesses want to keep you as a customer. If the problem isn't resolved, try writing to company headquarters. Describe exactly what the problem is, and include photocopies of any documents involved. You can also try any of the following, depending on the nature of the problem:

Better Business Bureau

Call the Better Business Bureau (BBB) in your locality. BBBs are associations of businesses that support efforts to keep all businesses honest. Although a BBB cannot force a business to do anything, it can formally notify a business of a complaint and seek an explanation. Some businesses settle disputes quickly

so complaints will not become part of their permanent file at the BBB. BBBs in Illinois can be found at:

www.bbb.org/us/il

Third-party dispute resolution programs

Several industries have programs to help resolve disputes between consumers and manufacturers. If you have contacted the seller and maker of a product without success, one of these programs may help. Check the information on warranties and service that came with the product to see whether it lists such a program.

Illinois Attorney General

The Illinois Attorney General's office handles complaints of violations of Illinois consumer protection laws. The Office's Consumer Protection Division can be contacted at these numbers:

Chicago
(800) 386-5438

Springfield
(800) 243-0618

Carbondale
(800) 243-0607

You can download a fillable Consumer Complaint Form at:

https://illinoisattorneygeneral.gov/consumers/index.html

and send it to the Attorney General at the address on the form. Your complaint will be examined by members of the Attorney General's staff. It may be forwarded to other government agencies, and to the person or entity you complain about. The complaint form is a public record. But the Attorney General's Office says that your identity will not be disclosed to anyone outside the Office.[76] The Attorney General also has a pamphlet with tips on how to avoid several types of consumer fraud (telemarketing,

home repair, charities, health care, and sweepstakes fraud), available at:

http://illinoisattorneygeneral.gov/consumers/consmalert0305.pdf

Small-claims court

You can sue for damages up to $10,000 in small-claims court.[77] You should call the court clerk to get information needed to file a claim. You usually do so by paying a small filing fee and filling in a short, simple complaint stating (1) your name, address, and phone number; (2) the defendant's name and residential or business address; and (3) the nature and amount of the claim, with any supporting evidence (including a copy of a written contract if there is one).[78] Your local small-claims court may be listed in your telephone directory under the name of your county, usually under the subheading "Circuit Clerk."

As is true in regular court, you are not required to hire a lawyer to present your own case in small-claims court. The judge can choose to hold an "informal hearing"—somewhat like those in television programs showing minor legal disputes between real persons—in which rules of procedure and evidence are relaxed. But it may be helpful to observe other cases in the local small-claims court, or to ask a lawyer for tips on what you need to know before the court date.

Regular court

If you have a claim for more than $10,000, you may want to sue in the regular courts. Although you are not actually required to be represented by a lawyer in regular court, it is highly advisable to get such representation. Of course, the cost of suing may exceed the amount of your claim. But if a number of people have essentially the same claim against one business, they may be able to file it as a "class action" and spread the costs among them. If you think you are one of many people who were defrauded, you can try to find some others to join you in such a suit.

Notes

Illinois laws cited below can be found in the Illinois Compiled Statutes (ILCS), Illinois' official code of laws. It is published by legal publishers and available online (at www.ilga.gov). A citation to a section of it looks like this: 815 ILCS 505/1. In that citation, "815" is the chapter number, "505" is the number of an act within that chapter, and "1" is the number of the first section of that act.

The Illinois Administrative Code (Ill. Adm. Code) and Code of Federal Regulations (Code of Fed. Regs.) are compilations of regulations issued by administrative agencies, which are also available online (at www.ilga.gov for the Illinois Administrative Code, and www.ecfr.gov for the Code of Federal Regulations).

A citation to federal law is in the form "15 U.S. Code sec. 6502" (Title 15 of U.S. Code, section 6502). Your local library may have a bound version of the U.S. Code. Sections of it can be viewed at: http://uscode.house.gov

Other abbreviations used in these notes are:

"sec." or "secs.": section or sections

"ff.": and the following sections

Endnotes

1. "National Do Not Call Registry FAQs" (revised May 2021), downloaded from FTC Internet site.
2. 16 Code of Fed. Regs. subsecs. 310.4(b)(1)(iii)(B)(2) and 310.2(q); "National Do Not Call Registry FAQs."
3. 325 ILCS 65/20.
4. Examples are "Real-World Passwords" (blog post), Dec. 14, 2006, downloaded from Schneier on Security Internet site, and "Millions using 123456 as password, security study finds" (BBC post), April 21, 2019, downloaded from BBC.com Internet site.
5. "The Dangers of Randomly Clicking Links," downloaded Dec. 7, 2022 from Fool Proof Me Internet site.
6. "How to Recognize and Avoid Phishing Scams" (revised Sept. 2022), downloaded from Federal Trade Commission Internet site.
7. 740 ILCS 7/10.
8. "How to Recognize, Remove, and Avoid Malware" (revised May 2021), downloaded from FTC Internet site.
9. "How To Spot, Avoid, and Report Tech Support Scams" (revised Sept. 2022), downloaded from FTC Internet site.
10. "How to Get Less Spam in Your Email" (revised May 2021), downloaded from FTC Internet site.
11. 16 Code of Fed. Regs. secs. 435.1, 435.2, and 435.3.
12. 15 U.S. Code sec. 1666.
13. 815 ILCS 145/2(a); 15 U.S. Code subsec. 1643(a).
14. 15 U.S. Code sec. 1693g.
15. 815 ILCS 140/1b.
16. 15 U.S. Code subsec. 1681a(f).
17. 820 ILCS 70/10.
18. 15 U.S. Code subsec. 1681h(a)(1).
19. 15 U.S. Code subsec. 1681g(a).
20. 15 U.S. Code subsecs. 1681g(f)(8) and 1681j(f).
21. 15 U.S. Code subsec. 1681g(a)(3)(A).
22. 15 U.S. Code subsec. 1681j(a)(1)(A).

23. 15 U.S. Code subsec. 1681j(b).
24. 15 U.S. Code sec. 1681i.
25. 15 U.S. Code subsec. 1681j(f).
26. Illinois Attorney General, "Identity Theft Resource Guide for Illinois Consumers" (Jan. 2008), pp. 3-15, available on the Attorney General's Internet site.
27. 15 U.S. Code subsec. 1681c-1(a)(1)(B).
28. 720 ILCS 5/16-35(a).
29. 815 ILCS 505/2MM(n-5).
30. "Identity Theft Resource Guide for Illinois Consumers" at pp. 17-18.
31. "Keeping Children Safe Online" (Security Tip ST05-002, revised Sept. 2, 2021), downloaded from Department of Homeland Security, Cybersecurity & Infrastructure Security Agency Internet site.
32. Based in part on "Online Safety Tips for Kids" (fact sheet, undated), downloaded from Illinois Attorney General's Internet site.
33. Based in part on "Keeping Children Safe Online" and "Online Safety Tips for Parents" (fact sheet), downloaded from Illinois Attorney General's Internet site.
34. 15 U.S. Code secs. 6501 to 6506; Federal Trade Commission, "Implementing the Children's Online Privacy Protection Act: A Report to Congress (Feb. 2007), downloaded from Federal Trade Commission Internet site.
35. 47 U.S. Code subsecs. 254(h)(5)(A) and (6)(A).
36. 325 ILCS 65/20.
37. 105 ILCS 5/27-13.3(c).
38. 815 ILCS 405/1 ff.
39. 815 ILCS 375/1 ff.
40. 815 ILCS 405/3 and 405/5, and 815 ILCS 375/3 and 375/5.
41. See the terms defined in 815 ILCS 405/2.11 and 405/2.12, and 815 ILCS 375/2.9 and 375/2.10.
42. See 815 ILCS 405/26 and 375/20, and 810 ILCS 5/9-609.
43. 815 ILCS 405/26, second and third paragraphs.

44. 205 ILCS 740/9(a)(19)(A) and (D).
45. 205 ILCS 740/9(a)(14).
46. 205 ILCS 740/9(a)(16).
47. 205 ILCS 740/9(a)(17).
48. 205 ILCS 740/9(a)(20).
49. 205 ILCS 740/9(a)(21).
50. 205 ILCS 740/9.2(c).
51. 205 ILCS 740/9.2(c)(1) to (3).
52. 205 ILCS 740/9.3(a).
53. National Highway Traffic Safety Administration, "Ratings," downloaded Nov. 4, 2022 from NHTSA Internet site.
54. U.S. Office of Energy Efficiency & Renewable Energy, "Gasoline Vehicles: Learn More About the Label" and "Electric Vehicles: Learn More About the Label," downloaded Nov. 4, 2022 from EPA Internet site.
55. 815 ILCS 205/4a(f)(3).
56. Federal Trade Commission, "Financing or Leasing a Car," (July 2022), downloaded from FTC Internet site.
57. 215 ILCS 152/35.
58. 815 ILCS 380/1 ff.
59. 815 ILCS 380/3(b).
60. 815 ILCS 380/4(a).
61. 815 ILCS 380/3(h).
62. 815 ILCS 380/3.
63. 815 ILCS 380/6.
64. 815 ILCS 380/4(b).
65. 815 ILCS 505/2L.
66. 205 ILCS 635/1-1 ff.
67. 735 ILCS 5/15-1603(b)(1); but see also subsec. (b)(3).
68. 735 ILCS 5/15-1603(e).
69. 735 ILCS 5/15-1602, fourth sentence.
70. 765 ILCS 67/1 ff.
71. 765 ILCS 67/5 (see definitions of "Dwelling structure," "Installment sales contract," "Residential real estate," and "Seller").

72. 765 ILCS 67/10(c).
73. 765 ILCS 67/20.
74. 765 ILCS 67/40.
75. 765 ILCS 67/10 and 67/70.
76. Illinois Attorney General's office, "Filing a Consumer Complaint," downloaded Jan. 27, 2023 from Attorney General's Internet site.
77. Illinois Supreme Court Rules 281 to 289.
78. Illinois Supreme Court Rule 282.

COMMISSION OVERVIEW

The Commission on Government Forecasting & Accountability is a bipartisan legislative support service agency responsible for advising the Illinois General Assembly on economic and fiscal policy issues and for providing objective policy research for legislators and legislative staff. The Commission's board is comprised of twelve legislators—split evenly between the House and Senate and between Democrats and Republicans. Effective December 10, 2018, pursuant to P.A. 100-1148 the former Legislative Research Unit was merged into the Commission.

The Commission has three internal units—Revenue, Pensions, and Research, each of which has a staff of analysts and researchers who analyze policy proposals, legislation, state revenues & expenditures, and benefit programs, and who provide research services to members and staff of the General Assembly. The Commission's staff fulfills the statutory obligations set forth in the Commission on Government Forecasting and Accountability Act (25 ILCS 155/), the State Debt Impact Note Act (25 ILCS 65/), the Illinois Pension Code (40 ILCS 5/), the Pension Impact Note Act (25 ILCS 55/), the State Facilities Closure Act (30 ILCS 608/), the State Employees Group Insurance Act of 1971 (5 ILCS 375/), the Public Safety Employee Benefits Act (820 ILCS 320/), the Legislative Commission Reorganization Act of 1984 (25 ILCS 130/), and the Reports to the Commission on Government Forecasting and Accountability Act (25 ILCS 110/).

- The **Revenue Unit** issues an annual revenue estimate, reports monthly on the state's financial and economic condition, and prepares bill analyses and debt impact notes on proposed legislation having a financial impact on the State. The Unit publishes a number of statutorily mandated reports, as well as on-demand reports, including the *Monthly Briefing* newsletter and annually, the *Budget Summary*, *Capital Plan Analysis*, *Illinois Economic Forecast Report*, *Wagering in Illinois Update*, and *Liabilities of the State Employees' Group Insurance Program*, among others. The Unit's staff also fulfills the agency's obligations set forth in the State Facilities Closure Act.

- The **Pension Unit** prepares pension impact notes on proposed pension legislation and publishes several statutorily mandated reports including the *Financial Condition of the Illinois State Retirement Systems*, the *Financial Condition of Illinois Public Pension Systems* and the *Fiscal Analysis of the Downstate Police & Fire Pension Funds in Illinois*. The Unit's staff also fulfills the statutory responsibilities set forth in the Public Safety Employee Benefits Act.

- The **Research Unit** primarily performs research and provides information as may be requested by members of the General Assembly or legislative staffs. Additionally, the Unit maintains a research library and, per statute, collects information concerning state government and the general welfare of the state, examines the effects of constitutional provisions and previously enacted statutes, and considers public policy issues and questions of state-wide interest. Additionally, the Unit publishes *First Reading*, a quarterly newsletter which includes abstracts of annual reports or special studies from other state agencies, the *Illinois Tax Handbook for Legislators*, *Federal Funds to State Agencies*, various reports detailing appointments to State Boards and Commissions, the *1970 Illinois Constitution Annotated for Legislators*, the *Roster of Illinois Legislators*, and numerous special topic publications.

Consumer Laws