Your financial future starts right here, right now.
What's behind the Credit Smart Series?

Credit Safe is part of the Credit Smart Series. These booklets are designed to help you, as a student, establish financial management skills that will serve you well this year, in five years and throughout your life. Being Credit Smart is a "strategy for a lifetime."

The Credit Smart Series includes:

- Credit Basics
- Credit Reporting
- Credit Scoring
- Credit Safe
- Repairing Credit Problems
- Credit Card Basics

This book is intended to provide helpful and informative material on the subject matter covered. The organization responsible for this publication is not engaged in legal, accounting, or other professional services, by publishing this book. If any such assistance is required, a competent professional should be consulted. The organization will not be responsible for any liability, loss or risk incurred as a result of the use and application of any of the information contained in this book.
IDENTITY THEFT. IT'S SERIOUS BUSINESS.

We've all heard about identity theft. Yet we think about it as something that happens to other people, not to us. In reality, in just the past five years alone, millions of people have become victims of identity theft. People just like us. People who go to school or work at universities, financial institutions, government agencies, and private companies.

It's not something to be taken lightly.

The impact of identity theft can be quite devastating. It can take months to resolve the problems and can affect you for several years even after the fraudulent use of your identity has ended. It can also cost you considerable money.

Identity theft is a federal crime. It occurs when someone knowingly uses or transfers your personal information without lawful authority to commit or to aid/abet any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state/local law.

Many states have passed laws related to identity theft, as well. Like we said, it's serious stuff.

HOW DO THIEVES GET THEIR HANDS ON YOUR IDENTITY?

Identity thieves will use your name, address, Social Security Number (SSN), your bank or credit card numbers or other identifying information. They'll illegally obtain this personal information by rummaging through trash, taking your personal property, stealing your mail, re-directing your mail to another address and using personal information they find on the Internet.

They might steal your records directly or bribe an employee who has access to your information. They can also hack into a company's computer system.

After they have your information, thieves can wreak havoc on your finances. They can take your money, charge new purchases to your accounts, open new accounts under your name, take out loans, and even use your name if they're arrested.

AccessGroup.Org
SO HOW DO YOU KNOW YOU’VE BEEN ROBBED?

Here are some of the warning signs that you may be a victim of identity theft:

- If you’re not receiving bills or other mail when you think you should be.
- If you’re getting credit cards you didn’t apply for.
- If you’ve been denied credit or have received less favorable terms for no apparent reason.
- If you’ve received calls or letters from debt collectors about unpaid charges on purchases you didn’t make.

The government is trying to help.

The FACT (Fair and Accurate Credit Transactions) Act of 2003 provides a number of protections to consumers. It allows for you to receive free credit reports annually so you can see if anything is odd in your report. It’s also easier now to place a fraud alert and harder to make changes on any accounts that you may have. There are more steps required to prove who you are.

Companies who report derogatory information about your account to a consumer reporting agency must notify you of their report. And the FACT Act calls for mandatory notification by a creditor when they’re offering credit terms to you based on your credit report that are less favorable than the most favorable terms available to a substantial proportion of the customers they serve. In other words, if they’re treating you differently they need to let you know.
PROTECT YOURSELF!

Please, please take special care to protect your Social Security Number, your personal information, your credit, your computer and your mail.

About your Social Security Number.

Never carry items around with you that contain your SSN and ask your account holders not to use your SSN as your account number. For example, SSNs were used as ID numbers on medical insurance identification cards, but that practice has stopped. Check your ID card to make sure your SSN is not used. DO NOT have your SSN printed on your checks. And never provide your SSN to anyone unless you initiated the contact.

Guard your personal information.

- Breaking into a car is a common way for ID thieves to get the information they need. Never leave your wallet, purse, or checkbook unattended in your car. In fact, it’s a good practice to carry as little as possible in your wallet. Get credit cards with your picture on them and destroy cards that you no longer use.
- Never provide personal information over the phone unless you initiated the call.
- Shred sensitive papers and documents including all of your financial “garbage.” It’s not enough to just put it in recycling.
- Memorize your ATM password/PIN – never store it in your purse or wallet.

Protecting your credit.

Check your credit reports for accuracy at least once a year. There are three national consumer reporting agencies – Equifax, Experian and Trans Union – you can get one free report from each agency once every 12 months thanks to the FACT Act. Just go to AnnualCreditReport.com.
Look over your credit card statements carefully. Don’t just look at the bottom line. Scan your purchases to make sure that they all make sense. It’s also a good idea to keep a list of all your credit card numbers and contact information in a safe and secure place. That way you can quickly notify your account holders if you lose your wallet. It’s not a bad idea to keep photo copies of your cards in that secure location, as well.

And, call 1-888-5-OPT-OUT (1-888-567-8688) or go to OptOutPrescreen.com to get out of pre-approved credit card solicitations. Doing so will reduce the chances that someone else will get hold of a solicitation that was mailed to you and use it for fraudulent purposes.

**Now for your computer...**

There are also steps you should be taking to protect data that’s on your computer.

First, make sure you use firewall software to guard against viruses, spam and other problems. If and when you make online purchases make sure you use a secure browser. A secure site will have **https** (the “s” is important) in the URL. There should also be a small lock icon to indicate it is a secure site. In addition you might consider using a single credit card account for all of your online transactions. It will be easier to spot discrepancies.

**Never use your debit card online.** If your information is compromised, there is a $50 limit on your liability for unauthorized use of your credit card under current federal law. But there currently is no such legal protection for debit cards. So, fraudulent use of your debit card could end up costing you a lot more.

**Snail mail.**

Don’t forget your old fashioned mail. Make sure your mail gets delivered to a secure location. A P.O. box is perfect. Don’t put bill payments in an unlocked mailbox (like an “outgoing mail” bin). And shred, shred, shred. Cross-cut shred all sensitive papers before they go in the trash. This includes pre-approved credit card offers, checks, insurance benefit statements, bills, bank and credit card statements, and anything that has a barcode on it.
IF IT HAPPENS TO YOU.

So, what if, even despite your best efforts, you become a victim? The sooner you realize it the better. That’s why you need to monitor your account statements (electronically if possible) and review your credit reports at least once a year. But if it happens, here’s what you should do:

1. File a fraud alert with all three national consumer reporting agencies.
2. Close the affected accounts immediately.
3. File a police report.
4. File a complaint with the FTC online at: ftc.gov/idtheft.

The police report will help for insurance and legal purposes and a creditor may want a copy. The complaint you file with the FTC will allow them to track occurrences and help them with record keeping.

You should also document all contacts you have regarding the situation and obtain legal counsel, if needed. You may get to the point where you’ll want to take legal action.

BECOME EVEN SMARTER.

We invite you to find out even more about identity theft. The more you know, the better you can protect yourself and take action if anything should occur.

Go to ftc.gov/idtheft and download the Federal Trade Commission’s free publication called “Take Charge: Fighting Back Against Identity Theft.”

In addition to the FTC site, you can also gain valuable information by going to the Privacy Rights Clearinghouse (privacyrights.org) and the Identity Theft Resource Center (idtheftcenter.org).
Your financial future starts right here, right now.

Our mission at Access Group

For more than 25 years, Access Group has made higher education available to students as a nonprofit loan provider, financial literacy educator and loan servicer. We are proud to have successfully guided thousands of students, like you, through the financial aid process. Today, we are excited about and thoroughly committed to furthering our mission of providing financial support and solutions to help aspiring professionals achieve success.

This workbook and the full breadth of the WiseBorrower® Education Series are important tools designed to help students begin their careers on solid financial footing. It is all part of our ongoing commitment to provide resources, enhance financial literacy and support higher education administrators and students in and out of school.