

Prevent Identity Theft and Fraud

For Older Americans



FIRST
Commonwealth[®]
● *Time to be first.*[™]

fcbanking.com 800.711.BANK(2265)

For more information about FREE Community Financial Education, contact:

Anna Frank

First Commonwealth Financial Education Program Coordinator

724-465-1984

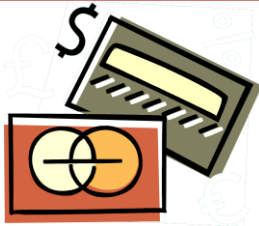
AFrank@fcbanking.com



fcbanking.com 800.711.BANK(2265)

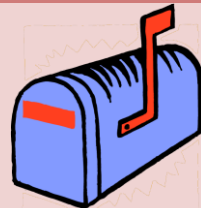
You could potentially be at risk for identity theft if you...

Use an ATM



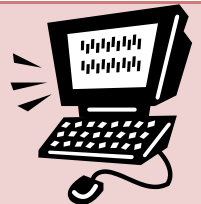
Pay for meal with credit card

Receive benefit checks in mail



Contribute to a charity

Do on line shopping / auctions



Do business over the phone

Write a check at the grocery store



It does not mean your identity WILL be stolen if you do any of the above activities. But you do have to be careful. Identity thieves and fraudsters can try to get your information ...

By Theft

- Mailbox
- Wallet or purse
- Your home
- Dumpsters
- Credit or debit card numbers by 'skimming'

From Businesses

- Stealing records while on the job
- Bribing an employee
- Hacking into computers
- Conning employees

Stealing your Credit Report

- Abusing employer's authorized access
- Impersonate your employer or landlord

On the phone/ Online

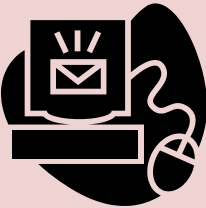
- Fake contest
- Fake magazine subscription
- Bogus "prize" that requires money
- Impersonate distressed family members
- Pretend to be a legitimate company that claims to have an issue with your account
- Misrepresentation on dating sites
- Over paying with bad checks for on-line auctions


How do thieves use personal information?



- ❖ Unauthorized credit card charges
- ❖ Apply for new credit in your name – credit card, store card, car loan, mortgage, etc.
- ❖ Establish phone service in your name
- ❖ Open bank account in your name
- ❖ File bankruptcy in your name
- ❖ Get ID in your name, with their picture
- ❖ Get a job in your name
- ❖ File tax returns in your name
- ❖ Give your name to police during an arrest

Tips for Fraud Protection


Online	Protection:
	<ul style="list-style-type: none">➤ Do NOT open email from unknown sources.➤ Be suspicious of any email urgently requesting financial information.➤ Under NO circumstances open email attachments unless the source is known and reliable.➤ Do NOT click on any links in emails from unknown sources.➤ ALWAYS look at the address Line at the top of an Internet Browser to verify that financial websites are legitimate.➤ Do NOT disclose any financial information online unless doing business with a known and trusted source.➤ Remember that legitimate companies will never ask for personal or confidential information in an unsecured email.➤ Regularly check bank, credit card and debit card statements to make sure all transactions are legitimate.➤ Do not use obvious passwords like your date of birth, your mother's maiden name, or the last four numbers of your social security number.➤ Never accept 'accidental' overpayments, with requests to wire back the balance for on line auctions.➤ Wait at least seven to ten days for checks to clear before mailing any products of an online auction.➤ Update virus protection software and firewalls regularly.➤ Do not use automatic log-in features that save your user name and passwords on a laptop.➤ Carefully read website privacy policies to be aware of how your information will be used or shared.➤ Forward suspicious emails to the Federal Trade Commission at spam@uce.gov

By Mail	Protection:
	<ul style="list-style-type: none"> ➤ Consider Direct Deposit for all regular payments to avoid having checks stolen from the mailbox. ➤ Carefully examine all letters and offers received through the mail, especially if it is not from a trusted source. ➤ Do NOT pay for 'free' gifts or prizes. ➤ Do NOT send money or provide financial information to anyone claiming to be a "lottery official". ➤ Do NOT send money or provide financial information to strangers promising a large sum of money for helping with money transfers. ➤ Be cautious when responding to promotions that are offered by mail. Research any business or company carefully before doing any business with them.

Other Tips



fcbanking.com 800.711.BANK(2265)

By Phone	Protection:
	<ul style="list-style-type: none"> ➤ Never give out personal or financial information over the phone, unless familiar with company. ➤ Ask for information to be mailed in writing when not sure if offer is legitimate. ➤ Do not fall for high pressure “act now” sales techniques. If the offer is legitimate, it will still be available tomorrow. ➤ Do not be afraid to hang up if an offer does not sound legitimate, or if not interested. ➤ Do not make donations to unknown charities. Check with the Better Business Bureau to see if organization complies with their standards

Other Tips

In Person



Protection:

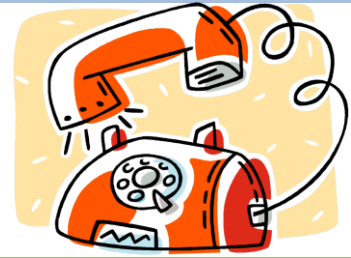
- There is a three day waiting period after some contracts are signed that allows consumers to cancel the contract without paying any fees.
- Do not make financial decisions when under stress or in a rush.
- Always get more than one estimate for home or other repairs.
- Take great care when using an ATM. DO NOT use the machine if it appears tampered with, or if suspicious characters are hanging around.
- Do not write your PIN number on the back of your ATM card or anywhere in your wallet or purse.
- Protect your social security number. Only give it out when absolutely necessary. Don't carry your Social Security card in your wallet.
- Keep your personal and financial information in a secure place at home. Never have it in an obvious place, especially if you have roommates, employ outside help, or are having work done in your home.
- Shred any personal or financial information before throwing it in the trash.
- Never wire money to an unknown person, business or charity.
- Carry only identification and credit and debit cards you will actually use when you go out.

Other Tips



fcbanking.com 800.711.BANK(2265)

The fine art of hanging up on people



Be alert when someone says...	Questions to ask	Actions to take
<p>“You have Won the lottery/ a contest!”</p>	<ul style="list-style-type: none"> ❖ When did I enter this lottery/ contest? ❖ Is there any fee associated with claiming this ‘prize’? 	<ul style="list-style-type: none"> ❖ Assume it is a scam until proven otherwise. Be extremely skeptical. If it sounds too good to be true, it is. Just hang up. ❖ If you think it might be a legitimate person, ask for a phone number where you can call them back. ❖ Hang up without giving out any personal information. ❖ Discuss it with a trusted family member before taking action. ❖ NEVER pay for a ‘prize’.

“Grandma, it’s your favorite grandson. You have to help me. I’ve been arrested. I need money. PLEASE don’t tell Mom or Dad!”

- ❖ What is your name?
- ❖ What is your mother’s name?
- ❖ Where are you?
- ❖ What did you do to get arrested?

- ❖ Verify that it is truly a grandchild in need.
- ❖ Decide if you can/want to help.
- ❖ Ask for name and phone number of jail/arresting officer.
- ❖ Hang up and call another family member to discuss issue.
- ❖ Do not make any rash decisions. If grandchild truly has been arrested, he/ she not going anywhere for a while.

“This is your bank/ other organization you do business with. There is a problem with your account. We need to verify your information. Please give us your name, social security number, birthdate and account number so we can check it against our records.”

- ❖ Don’t do anything.

- ❖ HANG UP! NO legitimate business will ever ask for this personal information over the phone.
- ❖ Do NOT give out ANY information, no matter how ‘urgent’ the caller might make it sound.



“We have a special offer just for you! If you act now, you can subscribe to this great magazine for a low, low price/ purchase this wonderful item for a low, low price!”



- ❖ Please send me the offer in writing.
- ❖ Is there a website I can visit?
- ❖ I am going to take some time to think it over. What number can I call if I decide to do business with you?

- ❖ Take some time and decide if magazine/ item is truly desired.
- ❖ Research the company by contacting the Better Business Bureau. (See information below.)
- ❖ If item is wanted, and company is legitimate, call company back and request to do business through the mail.
- ❖ Consider using a credit card to make purchases (and paying it off right away.) Using a credit card can offer additional protection.
- ❖ Do not be pressured into doing anything rash. If it is a legitimate offer, it will still be good tomorrow and the day after that.



fcbanking.com 800.711.BANK(2265)

“Won’t you help the victims of the recent earthquake/ flood/ other disaster?”



- ❖ Is your charity recognized by the IRS?
- ❖ How will this money be used to help the victims?
- ❖ Does your charity have a website?
- ❖ What is your name and contact information?
- ❖ Please send me information in writing.
- ❖ Is there a website I can visit?
- ❖ I am going to take some time to think it over. What number can I call if I decide to donate to your charity?
- ❖ Research charity by contacting Better Business Bureau and IRS. (See information below)
- ❖ Consider donating with a credit card (and paying it off right away). Using a credit card can offer additional protection.
- ❖ Do NOT give any account information over the phone.
- ❖ Look at your budget every month and decide how much you can and want to donate to reputable charities. Contact the charities yourself, and donate that way. If anyone else calls you for donations, politely decline and hang up.

Better Business Bureau:

www.BBB.org
 Phone: (412) 456-2700
 Email: info@pittsburgh.bbb.org

Wise Giving Alliance

703-276-0100
www.give.org

You may verify an organization's tax-exempt status and eligibility to receive tax-deductible charitable contributions by asking to see an organization's **IRS letter recognizing it as tax-exempt.** You may also confirm an organization's status by calling the IRS (toll-free) at 1-877-829-5500.



fcbanking.com 800.711.BANK(2265)

Signs of ID theft that require immediate attention

- 1 Bills that do not arrive as expected.
- 2 Unexpected credit cards or account statements
- 3 Denials of credit for no apparent reason
- 4 Calls or letters about purchases you did not make
- 5 Charges on your financial statements you do not recognize
- 6 Money missing from bank accounts
- 7 Receive a credit card that you did not apply for

Other Signs



fcbanking.com 800.711.BANK(2265)

How to detect signs of ID theft on...

... A bank statement

- ❖ A first warning sign will be if the statement does not show up at all. The ID thief changed the victims address at the bank so that the victim will not notice missing money or unauthorized transactions.
- ❖ Balance totals of accounts are less than they should be, or accounts have been drained.
- ❖ Unauthorized transactions, electronic or in person.
- ❖ Purchases you did not make.
- ❖ Checks you did not write.

... A credit card statement

- ❖ Did not get the statement.
- ❖ Unauthorized purchases
- ❖ Any changes in your personal information you did not request.
- ❖ Any balance transfers you did not request.
- ❖ Any cash advances you did not request.

... A credit report

- ❖ Any potentially negative public record items you that are not yours.
- ❖ Any potentially negative credit items that are not yours.
- ❖ Any collection activity items that are not yours.
- ❖ Any changes in your accounts in good standing that you did not initiate.
- ❖ Any new account in good standing you did not open.
- ❖ Any requests for your credit history that you did not initiate.
- ❖ Any changes in your personal information you did not make.



fcbanking.com 800.711.BANK(2265)

Immediate steps to take if ID theft is suspected

Fraud Alert

- Contact credit bureau to place Initial Fraud Alert on report

Close Accounts

- Contact Security or Fraud Department of all financial institutions/ businesses in writing
- Close accounts where compromise is suspected
- Open new accounts with new Personal Identification Numbers
- Ask for proof in writing after accounts have been closed.

Monitor

- Work with banks, stores and credit card companies to verify if any unauthorized activity occurred.
- Check credit report to see if any unauthorized accounts were opened or if anyone applied for credit in your name.
- If any unauthorized activity is reported, follow “Steps to take if ID theft did occur”.

Steps to take if ID theft did occur

Police Report

- Identity Theft Report
- Police Report
- Obtain proof from businesses

FTC Report

- Use printed FTC ID theft complaint to receive ID Theft Report
- FTC uses information to investigate ID Theft crimes
- Online: www.ftc.gov/idtheft
- Toll Free: 1-8-77-IDTHEFT
- By Mail: Identity Theft Clearing House, FTC. 600 Pennsylvania Ave, NW, Washington, DC 20580

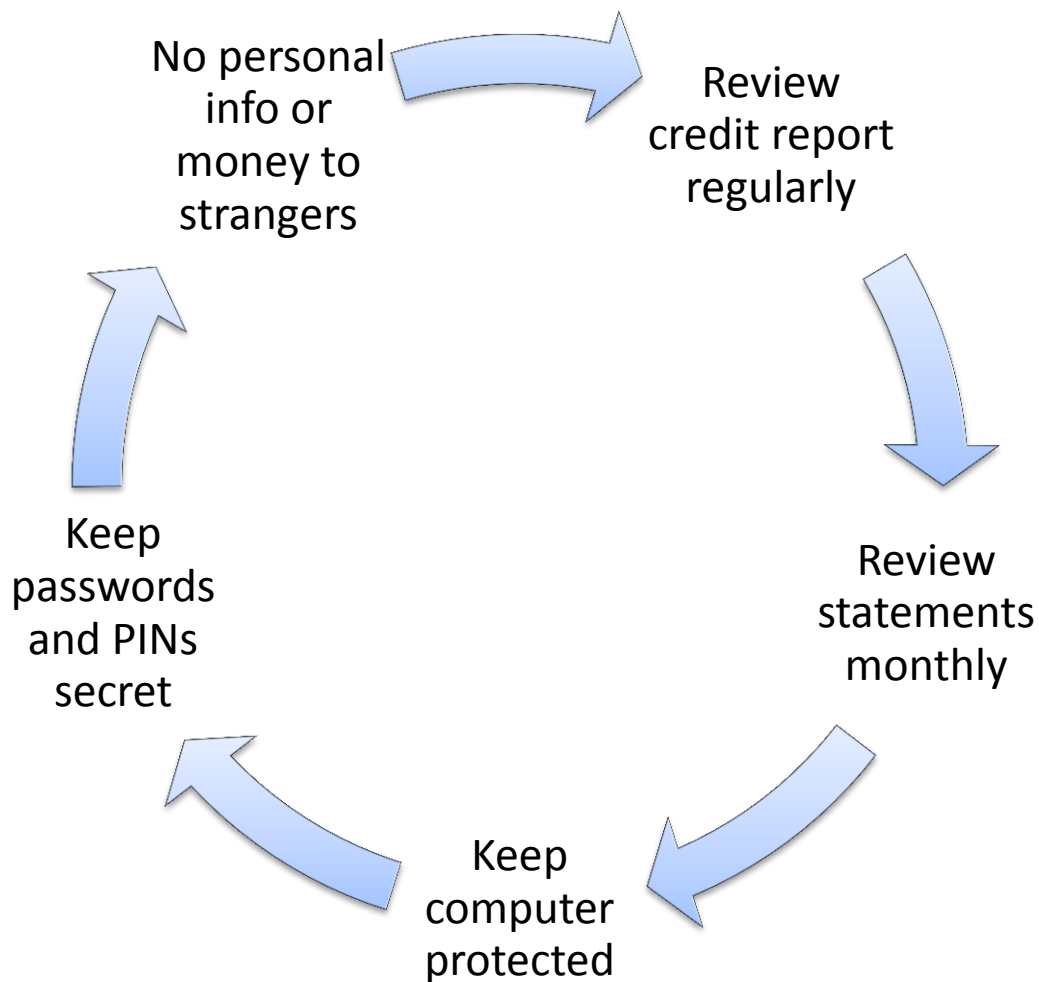
Resolve specific problems

- Bank accounts – work with security and fraud department. Ask for report in writing.
- Credit Report – work with credit bureaus..
- Credit Cards –Ask for report in writing.
- Criminal Violation – File impersonation report with police.



fcbanking.com 800.711.BANK(2265)

Remain ALERT!



Notes

Resources

www.fcbanking.com

www.ftc.gov

<http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm> - FTC Brochure: Take Charge: Fighting back against identity theft.

www.mymoney.gov

www.moneysbestfriend.com



fcbanking.com 800.711.BANK(2265)