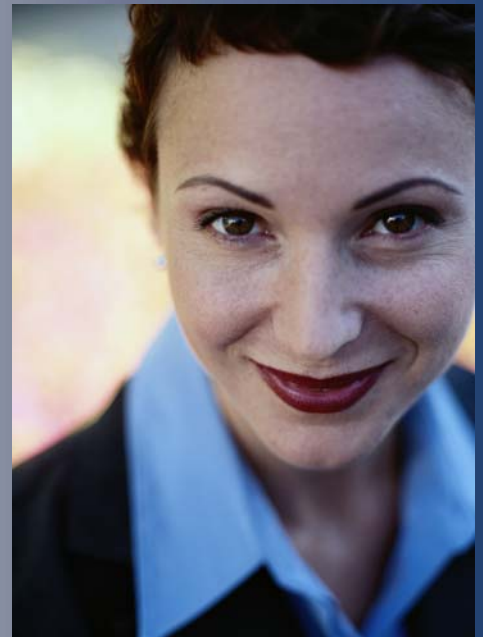




**Information to Protect Our Customers
From Identity Theft**





Information to Protect Our Customers from ID Theft

Identity (ID) Theft

Capital One understands that ID Theft is a growing concern of our customers, and that it is a frustrating experience for victims. We share these concerns and are striving to provide our customers with information to protect themselves from this crime. Thus, we have partnered with the Federal Trade Commission (FTC) to offer some helpful advice on how to tackle this issue.

ID theft is a very personal crime that occurs when someone uses information such as your name, Social Security Number, credit card number or other identifying information, without your permission, to commit fraud. ID Theft is one of the fastest growing crimes in the U.S.

How Does ID Theft Occur?

Here are some common methods that thieves employ to obtain your personal information:

Purse/Wallet Theft – They steal wallets and purses containing your identification, Social Security card, credit cards, ATM cards, and other personal information.

Mail Theft – They steal your mail including:

- bank and credit card statements
- pre-approved credit offers
- new checks
- tax information
- medical information

They target unattended mailboxes or complete a “change of address form” to divert your mail to another location.

“Dumpster Diving” – They rummage through your trash or the trash of businesses looking for personal data that they can use.

Inside Sources – They either have direct access to information in your home (i.e. friends, relatives, roommates, service providers) or access to businesses you work with that legitimately have your information.

Imposters – They pose as someone who has a valid need for personal information (i.e. businesses, government agencies, employer, landlord, etc.) and trick victims into divulging that information. They work their scams via:

- Telephone
- Look-alike Internet Websites
- Internet Pop-Up boxes
- Email

They can be so convincing that customers do not realize that they have been taken. For more details, see the “Phishing” section at the end of this document.





Information to Protect Our Customers from ID Theft

How Can a Thief Use Your Information?

Common types of identity theft are using another person's name to:

- Open and use credit card accounts.
- Write bad checks.
- Open various new accounts: i.e., checking, cell phone, gas, electric.
- Get personal or auto loans.
- Obtain employment.
- Rent an apartment.

It often takes some time for victims to realize that there is a problem. People whose identities have been stolen can spend months or even years (and their hard-earned money) cleaning up the mess that thieves have made of their good name and credit record.

How Can I Prevent ID Theft?

Review your credit report from the three major credit bureaus at least once a year.

Protect your credit cards

- Sign your credit card or write that the merchant must "check ID" on the back of the card.
- Close any accounts that you are not using.
- Make sure you receive your bills and review them for fraudulent charges.
- Place passwords on new or existing accounts.

Secure personal information in your home, especially if you have roommates, employ outside help or are having service work done in your home.

Keep your purse or wallet safe

- Secure your belongings at work.
- Guard your belongings in public places.
- Carry only identification and the credit or debit cards you actually need.

Safeguard your mail

- Do not leave outgoing checks in your mailbox. Use post office collection boxes instead.
- Request the post office to hold your mail if you are going to be on vacation by calling 1-800-275-8777.
- Call the issuing bank if you don't receive a check or credit card in the mail that you were expecting.

Shred your personal information

Do not throw away receipts, tax information, credit card offers, medical/insurance information, etc. without first shredding them.

Do not give out personal information over the phone, through the mail or over the Internet unless you have initiated the contact or are sure you know who you are dealing with.

Protect your Social Security Number (SSN)

- Do not carry your SSN card. Leave it in a secure place.
- Give your SSN only when absolutely necessary.
- If your state uses your SSN as your driver's license number, ask for a substitute number.

Protect your Personal Identification Numbers (PIN)

- Do not share your PIN with others.
- Be aware of others nearby when entering your PIN at an ATM machine.
- Do not write your PIN down.
- Do not choose a PIN that is easy to guess such as the part of your SSN or your date of birth.

Use extra care with personal information on your personal computer

- Avoid storing financial information on your PC.
- Update your virus protection software regularly.



Information to Protect Our Customers from ID Theft

What Should I Do If I Become a Victim of ID Theft?

There are 5 key steps that need to be taken immediately.

1. Call at least one of the three major credit bureaus (see chart below)

- Advise them that you have been an identity theft victim.
- Request a "fraud alert" and/or victim statement be placed on your credit file. This advises creditors to contact you personally before opening any new accounts in your name.
- When you place a fraud alert and victim statement with one bureau, all three bureaus will automatically be updated. (Note: Alerts and statements are removed after 90 days if you do not submit paperwork that the bureaus will send you.)
- Request a free copy of your credit bureau report. The credit bureaus must give you a free copy of your report if your file is inaccurate because of fraud.

Credit Bureau	Telephone Numbers	Address
TransUnion www.transunion.com	800-680-7289 Fraud Hotline	Email: fvad@transunion.com or write: Fraud Victim Assistance Dept P.O. Box 6790 Fullerton, CA 92834
Experian www.experian.com	888-397-3742 Fraud Hotline	P.O. Box 9532 Allen, TX 75013
Equifax www.equifax.com	800-525-6285 Fraud Hotline	P.O. Box 740241 Atlanta, GA 30374
Innovis www.innovis.com	800-540-2505 Fraud Hotline	P.O. Box 1373 Columbus OH 43216-1373

2. File a police report

- Call your local police department to file a police report. List any suspects that could have committed this crime.
- Request a copy of the police report. If you cannot obtain a copy, at least ask for the report number.
- Often the banks and creditors need proof of the crime in order to erase debts created by the identity theft.

3. Contact creditors

After reviewing your credit bureau reports, identify companies that:

- Manage your existing accounts that you suspect have been targeted by fraudsters.
- Opened new accounts that you did not request.
- Made inquiries on your credit bureau report when you did not request a loan.

Call every one of these companies and:

- ✓ Describe your identity theft problem.
- ✓ Tell them to close any new accounts that you did not open.
- ✓ If they made an inquiry, ask them **NOT** to approve any new loans that you did not request.
- ✓ If your existing account has been compromised, close that account and get a new account number.
- ✓ Ask for forms to:
 - Dispute any transactions that you did not make.
 - Report the fraud (a.k.a. an affidavit).
- ✓ Submit all forms in writing to get maximum protection. If the creditors do not provide forms, you can download sample dispute letters and affidavits from the FTC website at: <http://www.ftc.gov/bcp/edu/microsites/idtheft>



Information to Protect Our Customers from ID Theft

What Should I Do If I Become a Victim of ID Theft? (Continued)

4. Protect Your Bank Accounts

ATM: If your ATM card has been lost, stolen or compromised, we recommend that you:

- Immediately cancel your card.
- Request a new card with a new PIN.
- Request to have a password added to your account.

CHECKS: If your checks have been stolen or misused, call your bank and:

- Request a new account number.
- Place "stop payments" on any stolen checks.
- Ask your bank to contact their check verification service and instruct them to not accept the tampered checks.
- If needed, contact major check verification companies directly for additional services.

5. File a report with the Federal Trade Commission (FTC).

The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations.

There is a wealth of additional consumer information including a booklet called [ID Theft: When Bad Things Happen To Your Good Name](#) available by:

- Logging into the FTC website
<http://www.ftc.gov/bcp/edu/microsites/idtheft/>
- Calling the FTC toll-free at 1-877-ID-THEFT (1-877-438-4338).

Inform these check verification services of fraudulent activity on your checking account:

Telecheck	1-800-710-9898
Certegy, Inc.	1-800-437-5120
Checkrite/Global Payments	1-800-638-4600
ChexSystems/E-Funds	1-800-328-5121

Find out if bad checks have been passed using your name:

SCAN	1-800-262-7771
------	----------------





Information to Protect Our Customers from ID Theft

General Alert – “Phishing”

“Phishing” is an internet scam where the perpetrator sends out legitimate-looking emails or launches convincing pop-up boxes in an effort to fish for information from innocent victims. The fraudsters often link these emails and pop-up boxes to a replica of an existing Web page to trick a user into submitting personal, financial, or password data.

Recently, a few of our customers reported receiving deceptive e-mails claiming to be from Capital One. Here are a few tips to help you avoid this kind of scam:

1. **Do not reply** and **do not click on any links** in emails or pop-up boxes that request your personal information. “Phishing” criminals often use convincing lures to get you to reply such as:

- Threatening to close your account unless you provide personal information immediately.
- Claiming they need to update your personal records on your account.
- Offering a service if you give them your personal information to sign up.

Call the company that is attempting to contact you, using a trusted number, to make sure this is a valid request before you do anything. For example, if you get a suspicious Capital One email, you can contact us at the number on the back of your credit card and email suspicious emails claiming to be from Capital One to abuse@capitalone.com.

Often these emails and pop-up boxes link customers to “look-alike” web sites of legitimate businesses that are so realistic that they trick customers into thinking they are responding to a bona fide request. Unknowingly, customers submit their personal information to the criminal – not to the businesses.

2. Check for unauthorized charges in your bank and credit card statements as soon as you receive them. Also, if your statement is late by more than a couple of days, call to confirm the accuracy of your billing address and to review account transactions.
3. Help the government investigate the illegal activities of criminals by forwarding the actual phishing e-mail to the FTC at spam@uce.gov.



Information to Protect Our Customers from ID Theft

ID Theft Victim Action Log - It is very important for you to keep a record of your actions.

Credit Bureaus

Bureau	Phone Number	Date Contacted	Contact Person	Comments
TransUnion	1-800-680-7289			
Experian	1-888-397-3742			
Equifax	1-800-525-6285			
Innovis	1-800-540-2505			

Banks, Credit Card Issuers and Other Creditors

Company	Address and Phone Number	Date Contacted	Contact Person	Comments

Law Enforcement Agencies

Agency/Dept.	Phone Number	Date Contacted	Contact Person	Report Number	Comments
FTC	1-877-IDTHEFT (1-877-438-4338)				
Local Police Dept.					

Capital One issues this package of information as a service to our customers regardless of the outcome of any fraud investigation decisions. Receiving this information does not limit Capital One's ability to collect payment on charges that we determine are not fraud and are the responsibility of our cardholders.



P.O. Box 26074
Richmond, VA 23286