PROTECT YOURSELF AND YOUR IDENTITY

Chase Identity Theft Tool Kit

USE THESE IMPORTANT CONTACTS TO KEEP YOURSELF PROTECTED

CHASE CONTACTS

Customer Protection Group

Credit Cards	1-888-745-0091

Other Account Inquiries:

Debit Cards	1-800-935-9935
Deposit Customers	1-800-935-9935
Mortgage Customers	1-800-848-9136
Auto Loan Customers	1-800-336-6675
Auto Lease Customers	1-800-227-5151
Brokerage Clients	1-800-392-5749
Education Financing	1-800-489-5005
Home Equity Loan or Line of Credit	1-800-836-5656

www.chase.com/identitytheft

CREDIT REPORTING AGENCIES

Remember, you're entitled to a free credit report every year from each of the three major credit reporting agencies. Request yours today. More info is available at **www.annualcreditreport.com**.

Equifax	1-800-525-6285
Experian	1-888-397-3742
TransUnion	1-800-680-7289

OTHER IMPORTANT CONTACTS

Federal Trade Commission Identity Theft Information

To learn more about identity theft, visit the Federal Trade Commission consumer website at **https://www.identitytheft.gov/**, or call 1-877-ID-THEFT.

United States Postal Service

online at **https://postalinspectors.uspis.gov**

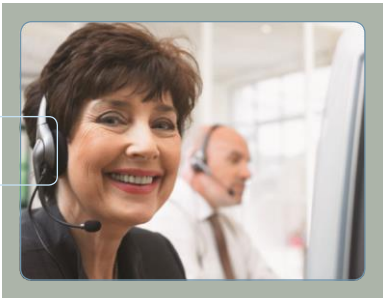
U.S. Secret Service

Find a field office near you at **www.secretservice.gov**

Social Security Number Fraud Hotline	1-800-269-0271
Social Security Department	1-800-772-1213
Lost or Stolen Passports	1-877-487-2778

At Chase, we work hard to provide customized tools and information to help

prepare you for whatever happens in your evolving financial life.



We've prepared this guide to help you defend yourself against identity theft. Use it to learn more about identity theft and the choices you can make to better protect yourself.

WHAT IS IDENTITY THEFT?

Identity theft happens when a criminal obtains your personal information to steal money from your accounts, open new credit cards, apply for loans, obtain services, and commit other crimes — all using your identity. These acts can damage your credit, leave you with unwanted bills and cause you countless hours and frustration to clear your good name.

This guide will help you understand identity theft and how to protect yourself from it. If you've already been a victim of identity theft, we'll give you an action plan to help you recover from

identity theft. We'll give you personal attention and work with you every step of the way. We'll also assist you as you work with credit reporting agencies and other key agencies.

DEALING WITH IDENTITY THEFT

Any time you think your identity has been compromised, be sure to contact the Customer Protection Group Call 1-888-745-0091.

If you've been a victim of identity theft, use this plan of action to recover from identity theft:

Contact the fraud departments of the three major credit bureaus (Equifax, Experian and TransUnion) – They maintain reports that track the credit accounts opened in your name.

- Request a consumer statement (victim statement) on your credit report that alerts creditors to call you before opening a new account or changing your existing accounts. You can attach up to 2 contact phone numbers and you can remove an alert at any time. **There are three types of alerts:**

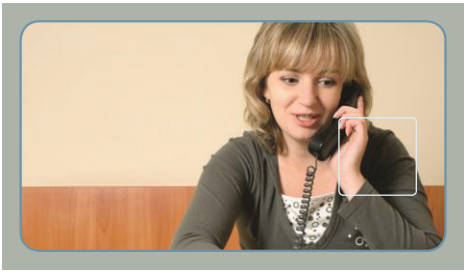
- An Initial Alert remains on file for 90 days (a decline remains on file for 90 days).
- An Extended Alert requires a law enforcement report and remains on file for 7 years (a decline remains on file for 5 years).
- An Active-Duty Alert is available to members of the military currently on active duty and remains on file for 1 year (a decline remains on file for 2 years).

You should call first and then follow up in writing when requesting alerts. See the sample credit reporting agency letters in the Sample Documents section.

- As a consumer, you're entitled to one free credit report every year from each of the three major credit reporting agencies (Equifax, Experian and TransUnion). Review your credit reports carefully and make sure that no additional fraudulent accounts were opened or unauthorized changes were made.
- Check the inquiry section of your credit report. When inquiries appear from companies that opened fraudulent accounts, request that the inquiries be removed from your report. Then follow up with the credit reporting agencies and any associated financial institutions.

Contact your local police –

File a report with your local police or the police in the community where the identity theft took place. A copy of the police report can help provide evidence of fraud to creditors. If the police cannot file a report, request that a miscellaneous incident report be filed. Remember an Extended Alert requires a law enforcement report.



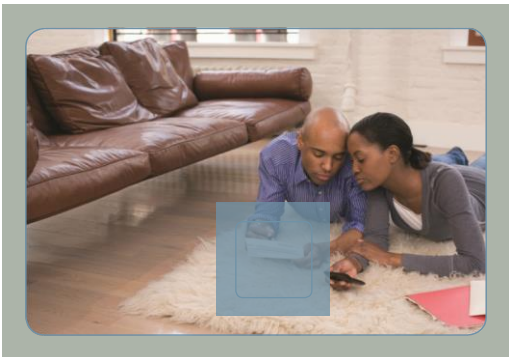
Perform periodic reviews to ensure accuracy –

- Review all accounts including credit card, bank, and utilities.
- Immediately report accounts that have been tampered with to the appropriate creditor, bank or utility. To contact the State Public Utilities Commission go to **www.fcc.gov/wcb/iatd/state_puc.html**
- Close accounts that have been tampered with and open new ones with new PINs and passwords. Avoid using easily available information as a password such as a birthday, Social Security Number, or mother's maiden name.
- If your checks were stolen or misused, close the account. Also, alert the major check verification

companies that you may be a victim to help them prevent further fraudulent use of your identity.

TeleCheck: 1-800-710-9898
Certegy: 1-800-437-5120

- If an identity thief has established a new phone or cellular service in your name, contact your service provider immediately to cancel the account. If you have trouble getting fraudulent phone charges removed from your account, contact the State Public Utilities Commission for local service providers or the Federal Communications Commission (1-888-CALL-FCC) for long distance service providers.



- If you believe someone is using your Social Security Number to apply for a job, contact the Social Security Fraud Hotline. Verify the accuracy of the earnings reported on your Social Security statement by contacting the Social Security Administration at 1-800-772-1213.

- If you suspect your name is being used by an identity thief to get a driver's license or ID card, or if your driver's license has been lost or stolen, contact your local Department of Motor Vehicles.

Evaluate and protect your computer –

If you identify hacking (the installation of malicious programs) or a computer virus alert the appropriate authorities by contacting:

1. Your Internet Service provider. The email address of a Internet Service provider can usually be found on their website.

2. The FBI at **www.ic3.gov**.

If you are a victim of Internet Fraud report it to the Federal Trade Commission, at **www.ftc.gov/complaint**. The FTC enters complaints into a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

If you get deceptive emails, including emails asking for your personal information, forward it to:

1. **spam@uce.gov**. Be sure to include as much information as possible.

2. **reportphishing@antiphishing.org**.
   The Anti-Phishing Working Group, is a consortium of Internet Service Providers, security vendors, financial institutions and law enforcement agencies.

If you have mistakenly given your personal information to a fraudster, file a complaint at **www.ftc.gov/complaint**, and then visit the Federal Trade Commission's Identity Theft website at **www.ftc.gov/idtheft** to learn how to minimize your risk of damage from a potential theft of your identity.

If you are suspicious about something on a social networking site, report concerns to the social networking site. Most sites have links where users can immediately report abusive, suspicious, or inappropriate online behavior.

Check mail carefully –

If you receive statements for accounts for which you did not apply, contact the creditor. If you don't receive statements for any of your usual accounts (including credit, banking and investment), contact the company immediately. If you don't receive mail you usually receive, contact the postmaster at your local post office. An identity thief may have falsified a change of address to redirect your mail to a different location.

SAMPLE DISPUTE LETTERS

If you're in the process of resolving identity theft and want to submit a dispute, use these proven letters as templates when corresponding with credit reporting agencies and credit card issuers. Be sure to provide the facts in a clear and concise manner and follow the other tips located in the Dealing with Identity Theft section.

Credit Reporting Agency

Date

Your Name
Your Address
Your City, State,
Zip

Complaint Dept.
Name of Credit Bureau
Address
City, State,
Zip

Dear Sir or Madam:

I am writing to dispute the following information in my file. The items I dispute are circled on the attached copy of the report I received. (Identify item(s) disputed by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)

This item is (inaccurate or incomplete) because (describe what is inaccurate or incomplete and why). I am requesting that the item be deleted (or request another specific change) to correct the information.

Enclosed are copies of (use this sentence if applicable and describe any enclosed documentation, such as payment records or court documents) supporting my position.

Please investigate this (these) matter(s) and (delete or correct) the disputed item(s) as soon as possible.

Sincerely,
Your Name

Enclosures: (List what you are enclosing)

SAMPLE DISPUTE LETTERS

Credit Card Issuers

Date

Your Name
Your Address
Your City, State,
Zip

Complaint Dept.
Name of Credit Bureau
Address
City, State,
Zip

Dear Sir or Madam:

I am writing to dispute a billing error in the amount of $_____ on my account. The amount is inaccurate because (describe the problem). I am requesting that the error be corrected, that any finance or other charges related to the disputed amount be credited as well, and that I receive an accurate statement.

Enclosed are copies of (use this sentence to describe any enclosed information, such as sales slips or payment records) supporting my position.

Please investigate this matter and correct the billing error as soon as possible.

Sincerely,
Your Name

Enclosures: (List what you are enclosing)

How Identity Theft Happens

No matter how careful you are about protecting your personal information, no one is completely safe from identity theft. Thieves can obtain your personal information in many ways.

In today's Wi-Fi, Internet-ready world, every website you establish an account with and every social media site you use could be a potential risk.

That's why it's so important to understand how identity theft happens.

Through Your Computer and the Internet

Phishing (pronounced "fishing") — You receive an email — which appears to be from a reputable company, asking you to respond or go to a website and provide your personal information. These emails may also contain fraudulent phone numbers to call to provide personal information – called *"vishing."* Remember, no legitimate representative of JPMorgan Chase will ever ask you for your PIN or password via email communication. They will request this information when you call in to discuss your account.

Spoofing — Setting up a bogus website that looks like a legitimate site and asks you to provide personal information.

Pharming — Redirecting your browser's request for a legitimate website to a bogus location that resembles it in order to collect your personal information.

Hacking — Using techniques to install malicious programs on your computer. The programs then capture your keystrokes and network traffic in order to steal personal information, including user IDs and passwords.

Stealing your laptop or smart phone — To use any unsecured data to discover passwords and access accounts.

Through Your Mail and Personal Documents

Stealing wallets and purses containing your identification, credit and bank cards.

Taking your mail, including bank and credit card statements, pre-approved credit offers, telephone calling cards and tax information.

Completing a "change of address form" to divert your mail to another location.

Rummaging through trash for personal data in a practice known as "dumpster diving."

Obtaining your credit report by posing as someone who may have a legitimate need for and a legal right to the information.

Finding personal information in your home.

How Identity Thieves Use Your Personal Information

They can call your credit card issuer pretending to be you, and change the mailing address on your credit card account, then run up charges on your account.

Because statements are sent to the new address, you may not realize there's a problem.

Thieves can open a new credit card account using your name, date of birth and Social Security Number. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report. They can establish phone or wireless service or open a bank account in your name, forge counterfeit checks or debit cards. They can even buy cars by taking out auto loans in your name.

HOW TO PREVENT IDENTITY THEFT

At Chase, we're committed to working with you to protect your personal information. We believe that one of the best ways to fight identity theft is to prevent it from happening in the first place. Here are some easy things you can do to prevent someone from stealing your information.

Carry only what you need.

The less personal information you carry, the better off you will be if your purse or wallet is stolen. For example, carrying your Social Security card with you is rarely necessary. Reminder: certain medical cards have your Social Security Number on them.

Don't put outgoing mail in your mailbox.

Drop your mail into a secure, official Postal Service collection box.

Report lost or stolen credit cards and checks immediately.

Review your account for unrecognized or counterfeit checks. Make sure the checks that clear the bank were written by you. Also, review new checks to make sure none have been stolen in transit.

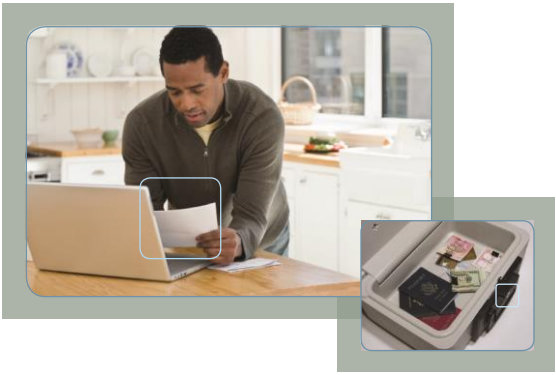
Don't preprint personal information on checks.

Your checks should not have your driver's license, telephone or Social Security Number on them.

Be alert to telephone scams.

Be wary about providing personal information. Notify the appropriate financial institutions of any suspicious phone inquiries made in their name asking for account information to "verify a statement" or "award a prize."

Conceal canceled, new and unused checks safely.



Be careful with your ATM and credit card receipts.

Never throw away receipts in a public trash can.

Guard your Personal Identification Numbers (PINs) and passwords.

Don't write your PIN on your ATM or credit cards and don't keep your PINs with your cards. Don't create PINs or passwords using information that can be guessed easily (birthdays, addresses, pets' names or your mother's maiden name). Don't share PINs or passwords with friends or family. Change your passwords often.

Discard mail appropriately.

Consider a home paper shredder for all sensitive documents. Shred financial solicitations that you're not interested in, bank statements, documents and invoices before disposing of them.

Keep your information private.

Do not give out personal or financial information such as checking account and credit card numbers – and especially your Social Security Number – on the phone unless you initiate the call or know the person or organization you're dealing with.

Keep track of monthly statements.

If regular statements fail to reach you, call the company to find out why. Someone may have filed a false change-of-address notice to divert your information to his or her address. If your statements include suspicious items, don't ignore them. Instead, investigate immediately and contact your bank or creditor to head off any possible or further fraud.

Try paperless statements.

In addition to cutting the amount of clutter in your home, paperless statements can also protect you against identity theft. Only you can view your

password protected statement on your financial institution's secure website.

Review your credit report.

Periodically contact the major credit reporting agencies to review your file and make certain the information is correct. You are eligible for one free credit report annually. For a small fee, you can obtain a copy of your credit report at any time. It's important to note that you can add a fraud alert message to your credit report that notifies potential credit grantors of their obligation to verify the legitimacy of a credit request made in your name.

Protect your computers.

A stolen computer or smart phone can provide a wealth of information to a thief. Learn how your device saves passwords and account numbers and be sure any software you use to store personal data is secure. Always set your laptop to require a password when it is turned on or awakened from sleep, especially when you're traveling.

Protect your identity online.

When conducting financial transactions, making purchases or sending personal information online, make sure the websites you visit are secure and protect your data from Internet theft. Look for websites that use Secure Socket Layer (SSL) technology to encrypt your personal information. You can also check to see if your web session is secure by looking for a small lock symbol usually located in the lower corner of your web browser window.

Current versions of leading web browsers indicate when a website is encrypted for transmission by using this symbol.

Another online safety feature is your password. Every time you log on to **www.chase.com**, you are required to enter your ID and password. For your safety, you should not reveal your password to anyone. For more information about how you are protected when using **www.chase.com**, or for more information about encryption, visit us at **www.chase.com**.

To speak to the
Customer Protection Group **call**
1-888-745-0091
www.chase.com/identitytheft

CHASE

BRC11606