CHASE IDENTITY THEFT PROTECTION KIT

Your security is important to us. Use this guide to learn more about identity theft, protect yourself, and recover if you have already been a victim.

To speak to our Customer Protection Group, call 1-888-745-0091; we accept operator relay calls.

WHAT IS IDENTITY THEFT?

Identity theft happens when a criminal gets your personal information and tries to steal money from your accounts, open new credit cards, apply for loans, rent apartments, and commit other crimes—all using your identity. Identity theft can damage your credit, leave you with unwanted bills, and require a lot of time and frustration to clean up.

REQUIREMENTS FOR REQUESTING CREDIT CARD DOCUMENTATION

We realize you may be a victim of Credit Card Identity Theft and would like details from a Credit Card application or account business records. Before we can send you specific details from any application or business record, we're required by the FACT Act of 2003 and our own identity protection policies to obtain the following information from you:

- A legible copy of a government-issued ID. We can accept a state-issued driver's license, a Military ID, a state ID card, or a passport.
- A signed and completed Identity Theft Report or Identity Theft Fraud and Forgery Declaration form. For your convenience, you can:
  - Complete the Identity Theft Report online at the website of the Federal Trade Commission (FTC) at identitytheft.gov.
  - Call 1-877-IDTHEFT (1-877-438-4338) to request the FTC Identity Theft Report.
  - Obtain an Identity Theft Fraud and Forgery Declaration form from your Chase branch or from any financial institution.
- A written request for a copy of the application that includes a summary of all relevant information about the identity theft.
- Third-party documentation, if applicable. Examples include approved Power of Attorney (POA), Conservator, Guardian, Trustee or Executor paperwork.

All written requests must be sent by First Class mail to:

Chase Card Services
ATTN: FACT Act Request
PO Box 15941
Wilmington, DE 19885-9918

HOW IDENTITY THEFT HAPPENS

Today, every internet-ready device and website you use could be a risk, especially when you set up or use accounts that require personal information.

Through Electronic Devices and the Internet

- Phishing (pronounced “fishing”) — You get an email that looks reputable but asks you to call a fraudulent number, respond to the email, or go to a website and enter personal information. Remember, no legitimate representative of JPMorgan Chase will ever ask you for your PIN or password by email. We will request that information only by phone.
- Spoofing — Bogus websites that look legitimate and ask you to provide personal information.
- Pharming — This can happen when you enter a legitimate website, but your browser is redirected to a bogus location that resembles it to collect your personal information.
- Hacking — There are many techniques thieves use to install malicious programs on your devices. The programs capture your keystrokes and network traffic to steal personal information, including user IDs and passwords.
- Stealing — If they get your laptop, smartphone, or another device, thieves can use any unsecured data to discover passwords and access accounts.
- Skimming — Obtaining credit and debit card numbers using a special device on ATMs or when processing a purchase.

Through Your Mail and Personal Documents

- Finding personal information in your home.
- Stealing wallets and purses with your identification 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, also 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.

HOW THIEVES USE YOUR PERSONAL INFORMATION

They can call your bank and change your mailing address
Thieves can pretend to be you and run up charges on your account. You may not know there’s a problem because statements are sent to the new address.

They can open new credit cards and bank accounts in your name
All they might need is your name, birthdate, and Social Security number (SSN). When they use the credit card and don’t pay the bills, the delinquent account is reported on your credit report.

They might also sign up for a phone or wireless service, forge counterfeit checks or debit cards, and buy cars by taking out auto loans in your name.

DEALING WITH IDENTITY THEFT

If you are a victim of identity theft, here’s how you can recover. For checklists and sample letters to guide you through the recovery process, go to IdentityTheft.gov.

1. Notify all your banks and financial companies as soon as you realize your identity has been stolen or an account is at risk.
    - If you bank with us, call our Customer Protection Group at 1-888-745-0091.

- We'll work with you to help correct any unauthorized transactions in your Chase accounts, fix any incorrect information we've sent to the credit reporting agencies and help protect you from any future identity theft or account fraud.

2. Ask the credit reporting agencies to place a fraud alert or credit freeze in your credit file. These agencies maintain the reports that track the credit accounts opened in your name.
    - A credit freeze, also known as a "security freeze," stops creditors from accessing your credit report. This makes it harder for identity thieves to open accounts in your name. That's because most creditors have to see your credit report to approve a new account.

3. Review your credit reports carefully.
    - You're entitled to one free credit report every year from each of the three major credit reporting agencies: Equifax, Experian, and TransUnion. Get more information and request yours today at AnnualCreditReport.com.
    - Look for all fraudulent accounts and unauthorized changes.
    - Check the inquiry section for fraudulent applications or accounts. If you see any, ask the agency to remove or mask the inquiry. A masked inquiry will only be visible to you.

4. File a report with local police, including the community where the identity theft took place.
    - You can give a copy to creditors as evidence of the fraud
    - If the police cannot file a theft report, ask them to file a miscellaneous incident report.

5. Report any issues with your mail and confirm your address.
    - If you receive statements for accounts you didn't open, contact the creditor.
    - If you don't receive statements for your usual accounts, contact the bank or other company.
    - If you don't receive regular mail, contact your local post office.

6. Close accounts that were opened, changed, or charged fraudulently. Review all your accounts, including credit cards, bank accounts, and utilities.
    - If you see suspicious activity, contact the creditor, bank or utility company.
    - If you open new accounts after that, use new PINs and passwords.
    - If checks were stolen or misused, tell the check verification companies.
        - TeleCheck: 1-800-710-9898
        - Certegy: 1-800-437-5120
    - If someone set up a new phone or wireless service in your name, ask the service provider to cancel the account. If they won't, contact the State Public Utilities Commission for local service providers or the Federal Communications Commission at FCC.gov. For long distance service providers, call 1-888-CALL-FCC (1-888-225-5322).
    - If someone used your SSN to apply for a job, call the Social Security Fraud Hotline at 1-800-269-0271. To confirm the accuracy of the earnings reported on your Social Security statement, call the Social Security Administration at 1-800-772-1213.
    - If someone used your name 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.

COMPUTER AND INTERNET FRAUD

If the fraud happened through your computer, here are some steps you can take.

If this happens	Here's what you can do
Hacking (the installation of malicious programs) and computer viruses	Contact your internet service provider and the FBI at IC3.gov.
Internet fraud	Report it to the Federal Trade Commission (FTC) at 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.
Deceptive or phishing emails	Forward them with any information you have to: • spam@uce.gov (FTC), and • reportphishing@antiphishing.org (The Anti-Phishing Working Group). If you see a suspicious email that appears to be from us, forward it to phishing@chase.com. We'll send you an automated response to let you know we got the message.
You gave your personal information to a fraudster by mistake	1. File a complaint at FTC.gov/complaint. 2. Go to FTC.gov/IDTheft to learn how to help reduce the damage of identity theft.
You're suspicious about a social networking site	Report concerns to the social networking site. Most have links where you can report abusive, suspicious, or inappropriate online behavior right away.

HOW TO PREVENT IDENTITY THEFT

One of the best ways to fight identity theft is to prevent it in the first place. Here are some ways you can help prevent someone from stealing your information.

Protect your devices	• Learn how your devices save passwords and account numbers. • Confirm that any software you use to store personal data is secure. • Set your laptop to require a password when it starts and wakes up.
Stay alert when you're online	• Make sure the websites you visit are secure and protect your data.

	• Look for websites that use Secure Socket Layer (SSL) technology to encrypt your personal information. Check for a small lock symbol  in the lower corner of your browser or next to the URL. • Set strong passwords and don't give them to anyone.
Watch out for telephone scams	• Keep your new, canceled, and unused checks private. • Don't give out personal or financial information over the phone, including checking account, credit card, and SSNs, unless you're sure the other party is legitimate. • Notify financial institutions of any suspicious phone calls that ask for account information.
Keep track of monthly statements	• If your statements don't reach you, call the company to find out why and confirm your address. • If your statements have suspicious items, don't ignore them. Investigate them right away and contact your bank or creditor.
Try paperless statements	These can protect you against identity theft and reduce your mail. Most sites will also ask for your password to view statements.
Check your credit report	• You're entitled to one free credit report every year from each of the three major credit reporting agencies. • You can also get a copy of your credit report anytime for a fee. • If you see suspicious accounts or inquiries, contact the agency.
Handle receipts and mail carefully	• Discard your mail safely. • Don't throw away ATM and credit card receipts in public trash cans. • Consider getting a paper shredder for sensitive documents like marketing offers, bank statements, documents, invoices, etc. • Use official postal service collection boxes for outgoing mail or secure your mailbox.
Be creative with your passwords and change them often	• The most secure passwords combine letters, numbers and special characters. • Never use your pet's name, your child's name or anything else that a fraudster could easily find out, like your address, phone number or birthdate. • Don't use information from your social media account for your password. • Avoid using the same password for multiple sites or financial institutions.

Guard your PINs and passwords	• Don't write your PIN on your ATM or credit cards. • Don't keep your PINs with your cards. • Don't share PINs or passwords with friends or family.
Carry only what you need	• The less personal information you carry, the better off you will be if your purse or wallet is stolen. • Check what you do carry, such as a medical card, for sensitive information like your SSN.
Report issues right away	• Report fraudulent activity, lost or stolen credit cards, and unrecognized checks. • Make sure checks that clear were written by you. • Review new checks to make sure none were stolen in transit.
Don't preprint personal information on checks	Your checks should not have your driver's license, telephone or SSN.
Be careful on social media	It's better to be cautious with the privacy settings and the personal information you share on social media.

IMPORTANT CONTACTS

Chase Contacts
Customer Protection Group: 1-888-745-0091
Website: chase.com/IdentityTheft

For other account questions:

Debit Cards	1-800-935-9935
Deposit Accounts	1-800-935-9935
Mortgages	1-800-848-9136
Auto Loans	1-800-336-6675
Auto Leases	1-800-227-5151
Brokerage Clients	1-800-392-5749
Education Financing	1-800-489-5005
Home Equity Lines of Credit	1-800-836-5656

We accept operator relay calls.

Credit Reporting Agencies

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

Other Important Contacts

Federal Trade Commission (FTC)	To learn more about identity theft, visit the FTC at FTC.gov/IDTheft or call 1-877-ID-THEFT (1-877-438-4338).
U.S. Postal Inspection Service	USPIS.gov
U.S. Secret Service	Find a field office near you at 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