

Identity Theft

Prevention and Recovery Information Kit

A step-by-step guide designed to help you protect your identity and recover if you've been victimized.

800-522-4100
valleynationalbank.com

Identity Theft... What is it?

At Valley, we feel it is important for you to be informed about identity theft and the related threats that face us as we go about our day-to-day activities. Identity theft is real; we are all potential victims and must safeguard our identities in order to reduce our exposure to this criminal behavior.

An identity thief steals identifying information (such as a Social Security number, date of birth, mother's maiden name, or a password) from an honest person and then uses that information to obtain credit cards, checking accounts, auto loans, telephone service, etc. in the honest person's name. Meanwhile, when the bills come for all the services they have obtained, the thief has abandoned the identity and the honest person is left trying to clear their name.

The employees of Valley National Bank are committed to aiding you in the fight against identity theft. By following the Bank's policies on information security and privacy, we will help keep our customers from becoming victims of this fast-growing crime. Additionally, as part of Valley's Identity Theft Program, specific procedures have been put in place to assist anyone who may already be a victim.

How do thieves steal an identity?

- They steal wallets and purses containing your identification and credit/bank cards.
- They steal your mail, including bank statements, pre-approved credit card offers, phone calling cards and tax information.
- They change your address with the post office to divert mail to another address.
- They "dumpster dive" - look through trash for personal information.
- They trick you into providing them with information by posing as a legitimate person on the phone (landlord, credit card representative, employer, etc.) or as a well-known company on the Internet (your bank, employer, etc.).
- They steal information you transmit over the Internet or that resides on your computer.

How can you tell that you may be a victim of identity theft?

Keep an eye out for the following signs:

- Unauthorized charges or withdrawals on any of your statements.
- Failure to receive bills or other mail as a result of an unwarranted address change.
- Upon review of your credit report, you notice loans or credit cards opened without your knowledge.
- Denial of credit for no apparent reason.
- Receiving calls or letters from debt collectors or companies on accounts you never opened.

Within this Information Kit, we provide you with precautionary measures you should take to protect your identity from being obtained by those with criminal intent. Also provided are step-by-step instructions for use if your personal information has been misused and forms that will help keep your records organized.

Protecting Your Identity

Follow the recommendations below to reduce the risk of your identity falling into the wrong hands.

How can you protect yourself against identity theft?

1. Avoid using easily obtainable information for passwords such as your mother's maiden name, your birth date, the last four digits of your Social Security number, or your phone number. Request to use another password instead.
2. Secure any personal information in your home.
3. Keep your Social Security card in a secure location and only give your Social Security number when necessary. If possible, attempt to use other types of identifiers.
4. Don't give out your personal information over the phone, through the mail, or over the internet unless you initiated the contact or are sure you know who you are dealing with.
5. Guard your mail and trash from theft by using only secured post office boxes for outgoing mail, and promptly remove mail from your mailbox after it has been delivered.
6. Shred charge receipts, copies of credit applications or offers, insurance forms, physician statements, checks and bank statements, and expired credit cards before throwing them out. Cross-cut shredders are preferred.
7. Report lost or stolen cards or checks immediately.
8. Cancel unused credit cards, and store cancelled checks securely.
9. Do not preprint personal information (driver's license #, telephone # or social security #) on your checks.
10. Limit your identification documents to those you need to carry. Do not carry your Social Security card in your wallet. Also, limit the number of credit and debit cards in your wallet to those you need.
11. Guard passwords and Personal Identification Numbers (PINs). Do not write them down in obvious places.
12. Utilize a firewall and antivirus software on your home computer.
13. Do not respond to unsolicited or unwanted email SPAM that may be requesting personal information to allegedly update or fill in "missing records" in your file.
14. Periodically review your credit report to ensure that it is correct. Requests can be made using the credit bureaus' contact information listed on the next page.
15. Let all three credit bureaus know you want to opt out of pre-approved credit offers by calling (888) 567-8688, or contact each of the bureaus listed on the next page.

Recovering Your Identity

If you are certain that your personal information has been obtained by someone you do not want to have it, act fast! It only takes a professional identity thief a matter of hours to cause enough damage to keep you busy for months, or even years, trying to rectify the situation. Below are a series of steps to follow immediately after you realize that you are a victim.

What do you do if you have been a victim of identity theft?

1. Place a fraud alert and/or freeze on your credit bureau file. This can prevent an identity thief from opening a new credit account or changing any of your existing accounts. The bureaus' contact information is below.

Equifax

Call toll free (800) 525-6285 or visit their website at www.equifax.com

Experian (formerly TRW)

Call toll free (888) 397-3742 or visit their website at www.experian.com

TransUnion

Call toll free (800) 680-7289 or visit their website at www.transunion.com

2. Additionally, notify ChexSystems (used by financial institutions as a source of information on your previous banking relationships) to place a fraud alert by calling (888) 478-6536.
3. Contact Valley National Bank either by calling our 24-hour Customer Service Center at (800) 522-4100 or by visiting one of our local branches.
4. Review all your accounts regularly (credit, bank and investment).
5. Complete an **ID Theft Affidavit** (located on page 6) and keep it readily available.
6. File a police report. Give them as much documented evidence as possible. Be sure the report lists the fraudulent accounts (if any).
7. Contact the Federal Trade Commission – (877) 438-4338 or (877) ID THEFT.
8. Notify your local Postmaster that your identity has been compromised. Request that no change-of-address request be granted unless you appear in person with two forms of identification.
9. If your Social Security number was misused, contact the Social Security Administration's Fraud Hotline – (800) 269-0271.
10. If you believe your driver's license has been misused, contact your local DMV (Department of Motor Vehicles) to place a fraud alert on your license and request a new driver's license number.
11. If you believe someone may have stolen your identity to file Federal income tax returns, call the Internal Revenue Service at (800) 829-0433.
12. Keep well-detailed records of every contact person you speak to about clearing your name. Using a **Contact Sheet** (located on page 5) may be helpful. Send all correspondence by certified mail with return-receipt requested. Keep copies of all documents and letters.
13. Periodically review your credit report for inaccuracies. You are entitled to one free credit report annually from each of the three major credit bureaus. For a free report visit www.annualcreditreport.com.

For additional information on identity theft, go to the Federal Trade Commission's web site at www.FTC.gov/idtheft

Credit Bureau	Phone Number	Contact Date	Contact Person	Comments
Equifax	800-525-6285			
TransUnion	800-680-7289			
Experian	888-397-3742			

Other Important Numbers	Phone Number	Contact Date	Contact Person	Comments
FTC ID Theft Hotline	877-438-4338			
Local Police Dept.				
ChexSystems	888-478-6536			
Social Sec. Fraud Hotline	800-269-0271			
Internal Revenue Service	800-829-0433			
Your State's DMV				

Financial Institutions	Phone Number	Contact Date	Contact Person	Comments
Valley National Bank	800-522-4100			

Creditors	Phone Number	Contact Date	Contact Person	Comments

ID Theft Affidavit

Name: _____ **Phone number:** _____

1. My full legal name is:

(First) (Middle) (Last) (Jr., Sr., III)

2. (If different from above) When the events described in this affidavit took place, I was known as:

(First) (Middle) (Last) (Jr., Sr., III)

5. My driver's license or identification card state and number are:

(State) (Number)

6. My current address is:

(Street) (City) (State) (Zip Code)

7. I have lived at this address since _____ (month/year).

8. (If different from above) When the events described in this affidavit took place, my address was:

(Street) (City) (State) (Zip Code)

9. I lived at the address in Item 8 from _____ until _____
(month/year) (month/year)

10. My daytime telephone number is () _____

My evening telephone number is () _____

How the Fraud Occured

Name: _____ Phone number: _____

Check all that apply for items 11 - 16:

11. I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.
12. I did not receive any benefit, money, goods or services as a result of the events described in this report.
13. My identification documents (for example, credit cards; birth certificate; driver's license; Social Security card; etc.) were:
 stolen lost on or about _____
(day/month/year)
14. To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization (If you do not know any of the below requested information, leave blank):

Name _____

Name _____

Address _____

Address _____

Phone number(s) _____

Phone number(s) _____

Additional information

Additional information

15. I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.
16. Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.) (Attach additional pages as necessary.)

Victim's Law Enforcement Actions

Name: _____ Phone number: _____

17. (Check all that apply) I have have not reported the events described in this affidavit to the police or other law enforcement agency.

The police did did not write a report. In the event you have contacted the police or other law enforcement agency, please complete additional pages as necessary.)

Agency #1

Officer/Agency personnel

Date of report

Report number, if any

Phone number

E-mail address

Agency #2

Officer/Agency personnel

Date of report

Report number, if any

Phone number

E-mail address

Documentation Checklist

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

18. A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.
19. Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).
20. A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Signature

Name: _____ **Phone number:** _____

I declare under penalty of perjury that the information I have provided in this affidavit is true and correct to the best of my knowledge.

(Signature)

(Date signed)

Knowingly submitting false information on this form could subject you to criminal prosecution for perjury.

(Notary)

Fraudulent Account Statement

Completing this Statement

- Make as many copies of this page as you need. **Complete a separate page for each company you're notifying and only send it to that company.** Include a copy of your signed affidavit.
- List only the account(s) you're disputing with the company receiving this form. **See the example below.**
- If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (**NOT** the original).

I declare (check all that apply):

- As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

Creditor Name / Address (the company that opened the account or provided the goods or services)	Account Number	Type of authorized credit / goods / services provided by creditor (if known)	Date issued or opened (if known)	Amount / Value provided (the amount charged or the cost of the goods/services)
Example: Example National Bank 22 Main Street Columbus, Ohio 22722	01234567-89	Auto Loan	01/05/2008	\$25,500.00

- During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing Address _____

Account Number _____