



The PBK Bank Identity Theft Kit is designed to give you some guidance as to the steps you might need to take if you find yourself a victim of Identity Theft. Steps to help prevent becoming a victim and ways that PBK Bank can assist you in avoiding Identity Theft are also included. This is in no way meant to be an all inclusive list but should prove to be a good starting point to assist you in recovering and protecting your good name.

## **If you are a victim of Identity Theft what should you do?**

### **1. Put a Fraud Alert on your credit report and review your credit report.**

Contact any of the three major credit bureaus to request a 90 day fraud alert to be added to your file. A fraud alert can help prevent any more fraudulent accounts being opened in your name. You only need to contact one of the three major credit bureaus, for they are required to contact the other two and place an alert for you.

Equifax: 1-800-525-6285

[www.equifax.com](http://www.equifax.com)

P.O. Box 740241

Atlanta, GA 30374-0241

Experian: 1-888-397-3742

[www.experian.com](http://www.experian.com)

P.O. Box 9532

Allen, TX 75013

TransUnion: 1-800-680-7289

[www.transunion.com](http://www.transunion.com)

Fraud Victim Assistance Division

P.O. Box 6790

Fullerton, CA 92834-6790

By placing a Fraud Alert on your account you are entitled to one free copy of your credit report from each company, and if you ask, only the last four digits of your Social Security number will appear on your credit report. Once you receive your credit report be sure to check it for accuracy and contact the reporting agencies to correct the data. Also, notice any accounts listed you've not opened and companies that have inquired on your credit report, as you may need to contact them.

### **2. Contact your bank (PBK Bank) and ask them to flag your accounts and close accounts if they have unusual activity.**

Close all accounts that have been affected by the Identity Theft and open new accounts to help stop the fraudulent activity. If fraudulent charges have been made to your accounts or new accounts opened in your name, but not by you, ask about disputing the charges to your account. You may also need to get a new ATM or Debit card issued to you and your old card may need to be closed.

The representative will be able to help you in tailoring the measures to take at the bank for your specific needs.

### **3. Contact the issuers of the credit cards you own.**

If unauthorized charges appear on your accounts or cards opened in your name without your authorization you may want to close your cards, request replacement cards with new account numbers, and monitor your credit card statements for additional fraudulent activity.

You may also want to check with any online accounts, merchants or payment services that you use for any fraudulent activity.

### **4. Contact your local police department.**

Some companies may require a police report to place Fraud Alerts on your accounts and to reimburse your account for fraudulent activity. Be prepared; as the police will have to prove that you are who you say you are so bring plenty of identification with you as well as proof of the crime.

## **5. File a complaint with the Federal Trade Commission.**

You can file a complaint with the FTC using their online complaint form (<http://www.consumer.gov>) ; call the FTC's Identity Theft Hotline 1-877-ID-THEFT (438-4338); or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Be sure to call the Hotline to update your complaint if you have additional information or problems. This will help law enforcement officials across the nation to track down identity thieves and stop them.

## **6. Contact the Social Security Administration.**

You need to contact the Social Security Administrations' Fraud Hotline 1-800-269-0271 to report the unauthorized use of your social security number.

## **7. Contact the Department of Motor Vehicles.**

By notifying the Department of Motor Vehicles you can find out if a license number had been issued in your name that you've not authorized.

## **8. Contact your local United States Postal Service.**

You can contact them in person or go through their website at [www.usps.com/websites/depart/inspect/](http://www.usps.com/websites/depart/inspect/) and file an "Identity Theft via US Mail" complaint form with the Postal Inspector.

## **9. Document your contacts and conversations.**

It is recommended that you document the names and phone numbers of everyone you speak to regarding your Identity Theft. Follow up your phone calls with letters and be sure to keep copies of all correspondence.

# **Steps to take to help prevent being a victim of Identity Theft**

## **1. Check your credit report frequently.**

You can get one free copy of your credit report every 12 months from each of the three major credit bureaus. To minimize the potential damage from Identity Theft, try spacing out when you get your credit reports. Instead of getting one from all three at the same time, try getting one from one then wait 3-4 months and then pull one from another credit bureau company and so on.

To get your free credit report you can visit [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or call 1-877-FACTACT (322-8128). Be sure to note that [www.annualcreditreport.com](http://www.annualcreditreport.com) is the official site setup between the credit bureaus and the national government.

## **2. Be careful with your mail.**

If you get junk mail, don't just toss it in the trash, be sure to shred or by some other means destroy your mail and documents with sensitive information on them. This will help to prevent people getting your personal information by going through your trash.

To opt out of prescreened list (aka junk mail) you can visit <https://www.optoutprescreen.com> or call 1-888-5-OPTOUT (1-888-567-8688). Opting out via the phone or internet will only opt you out of the prescreened list for 5 years.

## **3. Keep your important numbers in a safe place.**

It's important to keep important numbers such as your PIN, credit card, debit card, and checking account number in a secure location. If you were to lose your purse or wallet, would you have the numbers you need to call the companies to flag your accounts?

#### **4. Choose challenging Passwords**

It's recommended that you not use such things as your birthday, telephone number, or other such items as your password or PIN numbers.

You should also memorize your PIN and other important passwords (i.e. Internet Banking) and not share them with friends or family for added security.

#### **5. Protect your information.**

When conducting a transaction online, make sure the site is secure and reputable. Also, utilize anti-virus software and firewalls to help prevent hackers from stealing your information.

Always be sure to take your receipts from the ATM, gas pump and other stores.

Be sure to never give your confidential information, including your PIN, account numbers, passwords, and social security number to callers claiming they are from the bank or claiming that you have won a prize or to people you don't know.

#### **6. Beware of SPAM & Phishing scams.**

You should delete SPAM and Phishing emails, as they are simply trying to either steal your money, or your identity and then your money. To read "how to notice if an email is a scam" go to <http://onguardonline.gov/spam.html>.

### **How does PBK Bank help you to protect your Identity?**

#### **1. PBK Club Accounts**

With all Club Accounts through PBK Bank, you receive Personal Internet & Identity Coverage (Not a Deposit), and Lost Credit Card Notification. The Personal Internet & Identity Coverage helps you clear your good name, by giving you money up to \$5,000 per account per policy period for expenses incurred in clearing up you Identity Theft (Lost wages \$500 per week for four weeks max.)

Just because the transactions on your various accounts may be fraudulent and you are to get your money back from those charges in most cases, you usually don't get the money right away. Companies usually research the issue which can take weeks, before you have a chance of getting your money back. The Personal Internet & Identity Coverage helps fill in the gaps in the mean time, as your real bills don't stop coming.

The Lost Credit Card Notification is a 24 hour service that can allow you to report all of your cards (assuming you've gone to the process of entering in the information) by calling one number (1-866-210-0361 (toll free)).

*Please refer to your Master Policy for complete coverage details on the Personal Internet & Identity Coverage.*

#### **2. Enhanced Login Security on Internet Banking**

PBK Bank has added Enhanced Login Security to its Internet Banking product to give you peace of mind when viewing your Internet Banking. With Enhanced Login Security, you don't just log in with your password, but Internet Banking recognizes your computer for added protection and is yet another line of defense PBK Bank offers it's customers in the fight against Identity Theft.

#### **3. Verified by VISA**

Verified by VISA is a free service that PBK Bank offers to its card holders. When shopping on-line with Verified by VISA you get added protection against Identity Theft. When you shop at stores that participate you have to enter in a password before the transaction is valid. So if someone stole your card number, they would have to know your password as well before they could make their fraudulent purchase.

**4. PBK Bank offers several recourses to better educate you on how to prevent Identity Theft.**

On our website [www.pbkbank.com](http://www.pbkbank.com) you will find links too many great consumer protection recourses with links to the National Recourse about Identity Theft site, which is created by the Federal Trade Commission, and a link to the OnGuard Online “Your Safety Net” site created by several federal government agencies and the technology industry. We also offer other information on Identity Theft through such thinks as the Identity Theft Kit and various pamphlets available at any of our locations.