



# RICHARD CORDRAY

OHIO ATTORNEY GENERAL



## IDENTITY THEFT REPAIR KIT

SUBJECT:  
Identity Theft

BROUGHT TO YOU BY:  
Ohio Attorney General  
Richard Cordray

WARNING: | fastest growing white-collar  
crime in the US



## Message from Ohio Attorney General

Richard Cordray



Dear Friends,

Technology is a very important aspect of today's culture and society. It has led to many extraordinary discoveries from new planets to computers more advanced than we had ever dreamed. The downside to this growth of technology is the growth of new crimes. One that grows more and more each day is identity theft.

Anyone can be a victim of this crime. Even worse is the fact that a victim may not even know what is happening to them. That is why it is very important that you know how to protect yourself and combat identity theft if it happens to you. The aim of this handbook is to arm you with the tools you need to do just that.

The effects of identity theft can be devastating. It is vital for you to take action to correct the damage. Use this handbook to guide you through the steps of repairing the damage done by identity theft and preventing identity theft from happening in the future.

*Richard Cordray*

## Table of Contents

<b>INTRODUCTION</b>	<b>1</b>
What is Identity Theft?	2
How do they get my personal information?	3
What do they do with it?	3
Identifying Identity Theft	4
<b>WHEN YOUR IDENTITY IS STOLEN</b>	<b>7</b>
Immediate Response	
Step 1: File a Police Report	7
Step 2: Closing Accounts	7
Step 3: Fraud Alert	7
Step 4: Fixing Specific Problems	11
Step 5: File a Complaint/ID Theft Affidavit	16
<b>LIABILITY</b>	<b>19</b>
<b>CHECKLISTS</b>	<b>20</b>
Actions	
Documents	
<b>PREVENTING ID THEFT IN THE FUTURE</b>	<b>22</b>
<b>CONTACTS</b>	<b>24</b>

The information contained within this booklet is for educational purposes only and should not be substituted for the advice of an attorney licensed to practice law in Ohio.





**credit denied**

## WHAT HAPPENED?

You've just come home from a long day at work. The mail is here. More bills. It's just what you need after all the stress from a presentation that is already past deadline. You open your debit card statement. You didn't buy much this month – just some groceries and some clothes. Halfway up the driveway you stop. The statement shows an overdraft. You had more than \$1,000 in your checking account the last time you took out money and now you are more than \$50 in the negative.

You've finally saved up for a car. You've been waiting to get your very own car ever since you graduated from college. You've just picked out a beautiful little blue sports car and the salesman is off putting together the paperwork. Just as you are admiring what will soon be your new ride, the salesman comes up with a sad look on his face. "It's your credit," he says. "I'm sorry."

You finally found the perfect pair of shoes! You can't believe they have your size, too. You are positively beaming as you carry the box containing the precious shoes up to the cashier. It takes all of your self-control to not ask to wear them out of the store. The salesman rings you up, but there is a problem. Your credit card has been declined even though you hardly use it.

The police knock on your door. They have a search warrant. They inform you that your name, address, and phone number has been connected to a website containing child pornography. But you've never built a website and you only use your computer for balancing your checkbook and checking your email.

### *What happened?*

You are a victim of identity theft. Someone has obtained access to your checking account or stolen your debit card. Someone has ruined your credit history by opening credit accounts in your name that haven't been paid off. Someone has gotten a hold of your credit card number, either by stealing it, hijacking your computer, or by any number of other ways. Someone has used your personal information to conduct illegal activities. Now that your credit history is ruined and you are in debt for things you never knew about, you can't qualify for an auto loan to buy a car or pay for those perfect shoes. You could be in danger of being arrested for something you didn't do.

### **Now what?**



## WHAT IS IDENTITY THEFT?

Identity theft is when someone fraudulently uses your personal identification information to obtain credit, take out a loan, open accounts, get identification, or numerous other things that involve pretending to be you.

It is a very serious crime that can cause severe damage to someone's financial well-being if not taken care of promptly. People can spend months as well as thousands of dollars repairing the damage done to their credit history and their name by an identity thief.

Even scarier, some cases of identity theft are connected to other, more serious crimes which may lead law enforcement to you for a crime you did not commit.

## How Do They Get My Personal Information?

Identity thieves can obtain your personal information in a number of ways:

- > **Finding personal information you share on the Internet;**
- > **“Dumpster diving”** or going through your trash looking for personal information;
- > **Stealing your mail;**
- > **Stealing your wallet or purse;**
- > **Stealing your debit or credit card numbers through “skimming”**, using a data storage device to capture the information through an ATM machine or during an actual purchase;
- > **“Phishing”**: a scam in which the user sends an email falsely claiming to be from a legitimate organization, government agency, or bank in order to lure the victim into surrendering personal information such as a bank account number, credit card number, or passwords. This same sort of scam can also be done over the phone by the scammer calling your home;
- > **Obtaining your credit report** through posing as an employer or landlord;
- > **“Business record theft”**: involving the theft of files, hacking into electronic files, or bribing an employee for access to files at a business;
- > **Diverting your mail to another location** by filling out a “change of address” form.

## What Do They Do With It?

- > **Drain your bank account with electronic transfers, counterfeit checks, or your debit card;**
- > **Open a bank account in your name and write bad checks with it;**
- > **Open a credit card account that never gets paid off**, which gets reflected on your credit report;
- > **Use your name if they get arrested** so it goes on your record;
- > **Use your name for purchases involved in illegal activities**, such as products for methamphetamine production or an Internet domain for a child pornography site;
- > **Use your name to file for bankruptcy or avoid debts;**
- > **Obtain a driver’s license with your personal information;**
- > **Buy a car and use your information and credit history to get a loan for it;**
- > **Obtain services in your name**, such as phone, Internet or medical services.

## Identifying Identity Theft

Here are some warning signs that you may be the victim of identity theft:

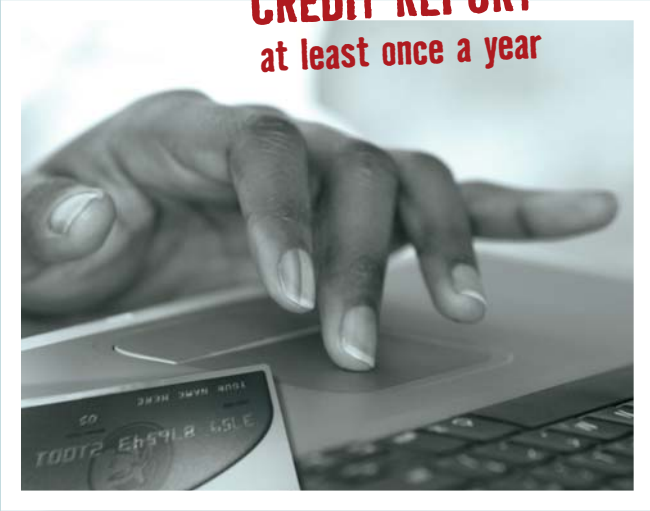
- You are denied credit;
- You find charges on your credit card that you don't remember making;
- Personal information, credit cards, insurance cards, ATM cards, checks, or IDs have been stolen from you;
- You suspect someone has fraudulently changed your mailing address;
- Your credit card bills stop coming;
- You find something wrong with your credit report, such as loans you didn't take out or accounts you don't remember opening;
- A debt collector calls about a debt you don't owe and didn't know about.

If any of these have happened to you, you may be the victim of identity theft.

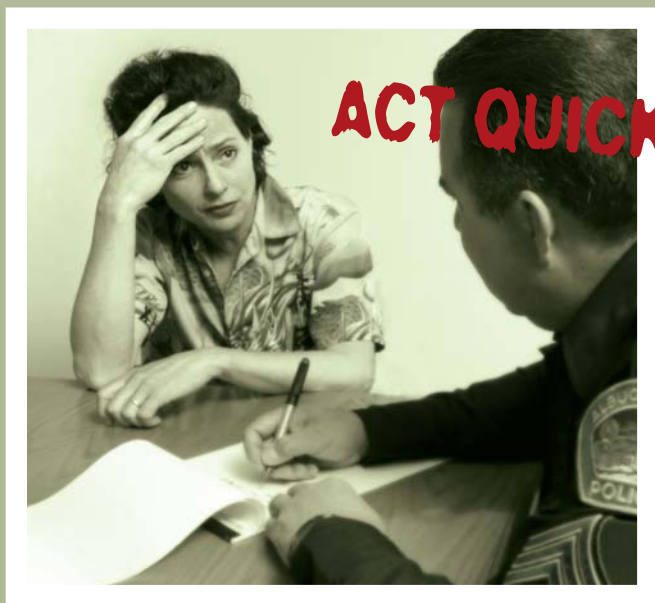
You could be the victim of identity theft without noticing any of these things happening to you, but it is still good to keep a careful eye out for anything out of the ordinary by ordering your credit report at least once a year and being alert to these warning signs.



**ORDER YOUR  
CREDIT REPORT**  
at least once a year



A free credit report is available  
at [www.annualcreditreport.com](http://www.annualcreditreport.com).



File a police report.

## WHEN YOUR IDENTITY IS STOLEN

There are steps you will need to take to protect yourself. You may have to spend some time and money dealing with having your identity stolen, but you will be okay. We are here to help you.

You have to follow these steps without hesitation. Acting quickly is the best way to make sure that this crime does not get out of control. The longer you wait, the more of your money someone else is spending and, potentially, the greater the damage to your credit.

**Always remember to act quickly.**

### STEP 1: CONTACT THE POLICE

File a report with your local police department and, if the identity theft did not take place within your area, file a report with the police from the area where the theft took place. Make sure to get a copy of the police report. You may need that documentation to support your claims to credit bureaus, creditors, debt collectors, or other companies. If you are unable to obtain a copy of the police report, be sure to get the report number.

### STEP 2: CLOSING ACCOUNTS

If you notice any accounts under your name that have been tampered with or opened without your consent, close them immediately. The longer that an identity thief has access to these accounts, the more money you

could lose. Call each bank or company and then follow up in writing. If there are fraudulent charges or debts on your account or if a new account has been opened, you should immediately file a fraud report with your bank's fraud department. If a new account has been opened without your knowledge and consent, ask the company with which the account has been opened if they have a fraud department. If they do, file a fraud report with that department. If not, ask if they will accept the ID Theft Affidavit from the Federal Trade Commission (see Step 6, page 16). If you close an existing bank account and open a new one, be sure to create a new PIN (Personal Identification Number) and password.

### STEP 3: FRAUD ALERT OR CREDIT FREEZE

The next step is to place a fraud alert on your credit file as well as review your credit report. This will prevent an identity thief from opening any more accounts in your name. You should contact the three major credit bureaus listed on page 8. If you place a fraud alert with one credit bureau, that credit bureau is required by law to contact the other two bureaus. The other bureaus will include the fraud alert in their reports. However, to ensure that the alert is included in your credit file as quickly as possible to minimize potential damage to your credit history you should contact all three credit bureaus immediately.

*Cont. on next page*

INITIAL FRAUD ALERT	EXTENDED FRAUD ALERT
<p><b>Lasts at least 90 days.</b></p> <p>It is good for when you suspect you might be a victim of identity theft, your wallet/purse is stolen, or if you are a victim of “phishing.” With an initial fraud alert, you are entitled to one free credit report from each consumer reporting company.</p>	<p><b>In your file for 7 years.</b></p> <p>You can get one on your credit report if you are a victim of identity theft and you have provided the credit bureau with an “Identity Theft Report.” This type of fraud alert also entitles you to two free credit reports from each credit bureau within 12 months.</p>

If you lose your Social Security card or think someone who should not have it has gotten a hold of it, contact a credit bureau and have an initial fraud alert placed on your credit reports.

### CREDIT BUREAUS

#### EQUIFAX

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

P.O. Box 740241  
Atlanta, GA 30374-0241  
1-800-525-6285

#### EXPERIAN

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

P.O. Box 9532  
Allen, TX 75013  
1-888-EXPERIAN (397-3742)

#### TRANSUNION

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

Fraud Victim Assistance Division  
P.O. Box 6790  
Fullerton, CA 92834-6790  
1-800-680-7289

After you have a fraud alert included in your credit history, you are entitled to receive a free copy of your credit reports from each of the credit bureaus. Request a copy and review your report for these things:

- Accounts you did not open;
- Debts on your account that you did not know about;
- Inquiries from companies you don't know;
- Inaccurate information.

Contact all three credit bureaus immediately.



#### STEP 4:

#### Apply for a PASSPORT

Immediately contact the police and file a police report. Ask your local law enforcement agency to enroll you in the Identity Theft Verification PASSPORT, a unique program created by the Ohio Attorney General's Office, which provides victims of identity theft a method of demonstrating to law enforcement and creditors that their identity has been stolen.

Once a law enforcement officer verifies the information in your report, they may wish to fill out a PASSPORT application on your behalf. The process is simple, the law enforcement officer will take your picture and fingerprints and ask you to sign the application. You will give the officer a phone number that you want to be used to activate your card. Then, the officer will submit the police report you filled out and send all the information to the Ohio Attorney General's Office.

Upon receipt, the Ohio Attorney General's Office will process the information and issue an Identity Theft Verification PASSPORT card to you.

Can you believe this is happening?



**STEP 5:**  
**Fixing Specific Problems**

You’ve identified the problems in your credit report as well as identity theft problems elsewhere. Now it is time to fix them. Here’s how:

*See CONTACTS on page 24 for contact information on these organizations.*

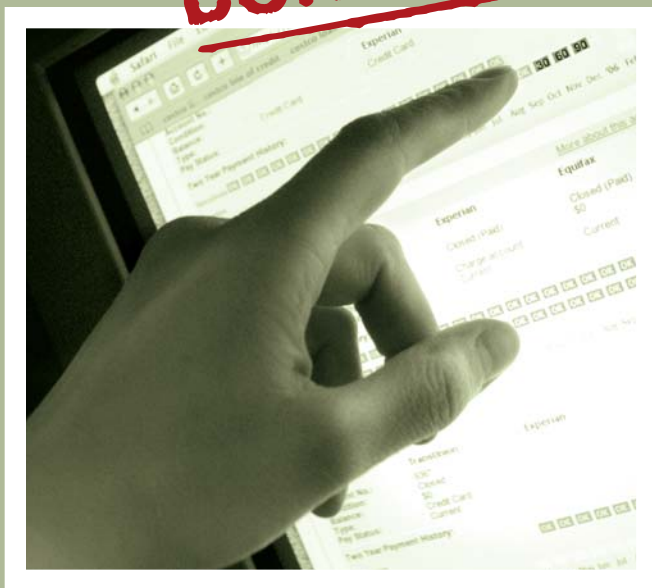
EVENT	ACTION REQUIRED	CONTACT
<b>You find any accounts tampered with or opened without your knowledge</b>	Close the accounts immediately. Get new passwords and PINs for new accounts.	Credit Bureaus and creditors (banks, credit card issuers), merchants, utility and cell phone companies
<b>Your ATM card, credit cards, or checks were stolen</b>	Close the accounts immediately. Get new PINs and passwords for new accounts. Notify each bank and major check verification companies. If your checks are stolen, put “stop-payments” on all checks remaining in the stolen checkbook. Ask any check verification company to put a fraud alert on your account.	Bank, credit card issuer, creditors, major check verification companies, and the police
<b>You find inquiries on your credit report that you did not know about</b>	By phone and then in writing, notify the three major credit bureaus that unauthorized credit inquiries on your credit history were made and request that those inquiries be removed.	Credit Bureaus
<b>You find inaccurate information on your credit report</b>	By phone and then in writing, notify the three major credit bureaus and request the information be corrected.	Credit Bureaus

*Cont. on next page*

EVENT	ACTION REQUIRED	CONTACT
<p><b>You have reason to believe your Social Security Number (SSN) has been stolen or misused</b></p>	<p>Report your allegations to the Social Security Administration (SSA), request a copy of your Social Security Statement, and/or call SSA to verify the accuracy of the earnings reported on your SSN.</p>	<p>Social Security Administration</p>
<p><b>An identity thief has falsified change-of-address forms, stolen your mail, or committed any other kind of mail fraud in order to get your personal information</b></p>	<p>Report it to your local post office. Contact your credit card companies, banks, etc. to notify them that your address was fraudulently changed. Have any changes of address done only in writing.</p>	<p>U.S. Postal Inspection Service (USPIS)</p>
<p><b>You've lost your passport, it was stolen, or you believe it is being misused</b></p>	<p>Contact the United States Department of State through a field office or on their website.</p>	<p>United States Department of State (USDS)</p>
<p><b>You think your name or SSN is being used to obtain a fake driver's license</b></p>	<p>Contact the Bureau of Motor Vehicles (BMV). Make sure you don't use your SSN as your driver's license number.</p>	<p>Bureau of Motor Vehicles (BMV)</p>
<p><b>You think an identity thief has interfered with your security investments or a brokerage account</b></p>	<p>Report it to your broker or account manager as soon as possible. File a complaint with the U.S. Securities and Exchange Commission.</p>	<p>Your broker/account manager, U.S. Securities and Exchange Commission</p>

EVENT	ACTION REQUIRED	CONTACT
<p><b>A phone service account has been opened in your name, someone is using your calling card, or unauthorized calls are being billed to your cellular phone</b></p>	<p>Cancel your account and/or calling card. Use new PINs if you open new accounts.</p>	<p>Your service provider</p>
<p><b>A debt collector contacts you trying to collect on a loan that you did not take out</b></p>	<p>Write a letter to the debt collector. State your reasons why you dispute the debt and include supporting documentation, such as a copy of the police report, or the FTC Identity Theft Affidavit.</p>	<p>Debt collector</p>
<p><b>You have been wrongfully accused of having committed a crime perpetrated by someone pretending to be you</b></p>	<p>File an impersonation report, have your identity confirmed, and prove your innocence by comparing your information to that of the identity thief.</p>	<p>You will possibly need the assistance of a lawyer, i.e., a criminal defense attorney (public or private) in order to clear your name. Contact the Public Defender's Office or the Ohio Bar Association in order to find an attorney.</p>
<p><b>You believe someone has filed for bankruptcy in your name</b></p>	<p>Write to the U.S. Trustee and include supporting documentation. File a complaint with the U.S. Attorney and/or the FBI.</p>	<p>U.S. Trustee in the region where the bankruptcy was filed, U.S. Attorney, FBI in the city the bankruptcy was filed, and you may want to contact the Public Defender's Office or the State Bar Association in order to find an attorney to help you.</p>
<p><b>You believe someone has used your medical benefits to obtain services</b></p>	<p>Report it to your insurance company and the medical provider.</p>	<p>Your medical provider. They will likely have internal protocol to follow.</p>

**DON'T WAIT**



You can check your credit report online immediately  
at [www.annualcreditreport.com](http://www.annualcreditreport.com).

## Getting Your Credit Report Fixed

If you find inquiries on your credit report that you did not know about, contact the credit bureau and request that those inquiries be removed. If you find inaccurate information, you must contact the credit bureau as well to have it fixed. First call them and then follow up in writing. Provide copies of documents for support. If you cannot get any documentation from the creditor, send the credit bureau copies of your police report. Clearly identify what information you are disputing. Once your credit report is corrected you can ask for the credit bureau to send notices of the corrections to anyone your credit report was sent to in the last six months.

## Creditors

If your credit card was stolen or you find fraudulent charges on your credit card bill, close the account immediately. Then contact the credit card company about the fraudulent charges. Make sure your letter includes your account number and a description of the unauthorized charges as well as your name and address. Send the creditor a copy of your police report and a copy of your ID Theft Affidavit (see page 16). If they do not accept the ID Theft Affidavit, fill out the creditor's fraud dispute forms. Request a return receipt so that you have proof of when the letter was received for your records as well as to show that the letter arrived within

the required 60 days after you received the bill with fraudulent charges. Even if the address on your account was changed, you must still notify the creditor in writing within 60 days after the bill would have reached you. Remember to keep track of your billing statements. If you do not notify the creditor within 60 days, you may be liable for the fraudulent charges.

*See Liability on page 19 for more information.*

## Social Security Number

If you continue to have problems with an identity thief misusing your Social Security Number, the Social Security Administration (SSA) can issue you a new number, but this is not guaranteed to solve your problems. It is even possible that getting a new SSN will create more problems. A new SSN does not guarantee a new credit record. Credit bureaus might combine your new SSN credit record with your old SSN credit record. Even if that does not happen, the absence of any credit history might make it harder for you to get credit.

Also, you cannot get a new SSN if:

- You lost your SSN card or it was stolen, but there is no evidence it is being misused;
- You filed for bankruptcy;
- You are planning on avoiding the law or legal responsibility.

## Criminal Violations

If an identity thief has impersonated you when they were arrested or cited for a crime, there are things you can do to correct your record. First of all, to prevent being wrongfully arrested, carry copies of documents showing that you are a victim of identity theft even if you do not know that criminal violations have been attributed to your name. If they have, contact the law enforcement agency (police or sheriff's department) that arrested the identity thief. Or if there is a warrant for arrest out for the impersonator, contact the court agency that issued it. You may want to get a lawyer to help you.

### **STEP 6:** **Filing Complaints**

The Federal Trade Commission is the federal consumer protection agency. The FTC, in conjunction with the FBI, maintains an Identity Theft Data Clearinghouse. The FTC aids identity theft investigations by collecting complaints from identity theft victims and sharing the information with law enforcement agencies, credit bureaus, companies where the fraud took place and other government agencies. File a complaint with the FTC by going to [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) or by calling their toll-free number: 1-877-ID-THEFT (1-877-438-4338).

## Identity Theft Affidavit

A piece of documentation you need to fill out is the Identity Theft Affidavit offered by the Federal Trade Commission. This form will help you report information about your identity theft with just one form. Many companies accept this form, though others will require you to use their own form or submit more forms. If a new account has been opened in your name, you can use this form to provide the information that will help companies investigate the fraud. Once you have filled out the ID Theft Affidavit as completely and accurately as possible, mail a copy to any of the companies concerned with the fraud you describe in the form, such as banks or creditors. The ID Theft Affidavit as well as more detailed information about filling it out can be found at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

Make sure that you keep copies of all of your paperwork including records of everyone you have corresponded with, fraudulent bills, police reports, and complaint forms.



**FILE**

**A COMPLAINT  
WITH THE FTC**

the **FASTER** you act  
**THE LESS**  
**LIABLE**  
**YOU ARE**



# LIABILITY

To ensure that you don't end up paying hundreds or even thousands of dollars in fraudulent charges made by an identity thief, the best course of action is to act quickly. The faster you act, the less liable you are for unauthorized charges.

## Credit Cards

According to the Truth in Lending Act, your liability is limited to \$50 in unauthorized credit card charges per card in most cases. In order for this to come into effect, however, you must write to the creditor within 60 days of receiving the first bill that contained the fraudulent charge. If an identity thief changed your mailing address, you must still send your letter within 60 days of when you were supposed to have received it. Keep track of your bills!

## ATM/Debit Cards

If your ATM or debit card is lost or stolen, report it as quickly as possible. If you report it within two business days, you are only responsible for \$50 in unauthorized withdrawals or transfers. If you report it between two and 60 days after, you may be responsible for up to \$500 in unauthorized withdrawals or transfers the thief may make. If you do not report it after 60 days, you can lose any money the thief withdraws or transfers from your account after the 60 days.

**report within 60 days**

# CHECKLISTS

## Plan of Action List

*Because this is a lot of information to take in, we have provided you with a checklist to go through to make sure you have taken all the necessary steps after becoming an identity theft victim. Remember, you must complete all of these steps in a timely manner so that the identity theft does not get worse and to minimize your losses.*

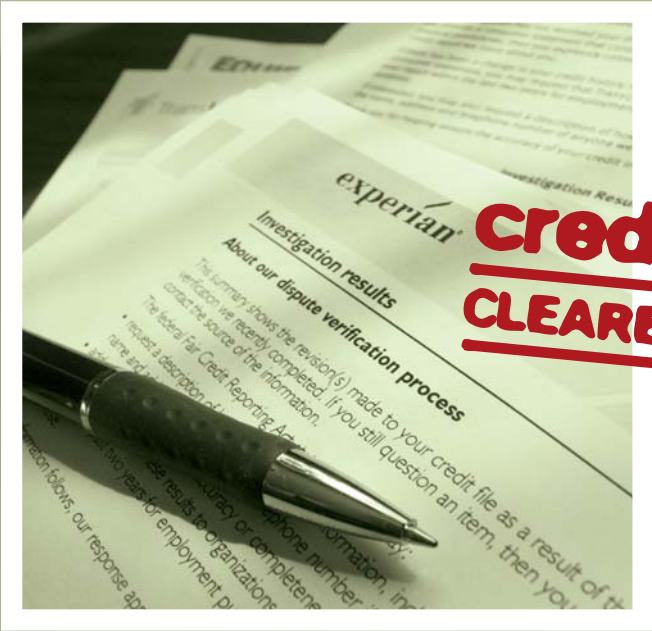
- 1. Filed a police report.
- 2. Obtained a copy of your credit report.
- 3. Identified errors, inquiries you did not know about, accounts you did not open, debts you did not know about, or anything else that seems wrong or out of place on your credit report.
- 4. Placed a fraud alert or credit freeze on your credit report.
- 5. Apply for an Identity Theft Verification PASSPORT.
- 6. Closed any accounts that might have been tampered with or opened without your knowledge or consent.
- 7. Contacted a major credit bureau by phone and by writing to correct inaccurate information.
- 8. Filled out the Identity Theft Affidavit.
- 9. Contacted the correct agencies to fix inaccurate information, close accounts, or report identity theft.
- 10. Filed a complaint with the Federal Trade Commission.

## Document List

*Here is a list of documents you should have. You won't be able to keep the originals of some of the documents so it is very important that you make a copy for yourself.*

*It is also a good idea to keep copies of the documents that prove you are an identity theft victim with you, such as a copy of your police report.*

- 1. Police report.
- 2. Identity Theft Affidavit.
- 3. Bills with fraudulent charges.
- 4. Documentation of accounts opened in your name without your consent.
- 5. Copies of letters sent to credit bureaus and creditors.



# PREVENTING ID THEFT in the future

*No matter how many precautions you take, identity thieves can find a way to steal your identity. But there are precautions you can take to minimize your risk for identity theft and can also help you catch identity theft quickly.*

- 1 Place passwords on bank, credit card, and phone accounts:** Don't use a password that could be easily guessed, such as your pet's name or your birth date and choose a password that mixes random numbers with letters.
- 2 Don't carry your Social Security Card:** Don't even carry the number on you. Don't use it as your driver's license number either. Keep the card in a safe place and use the number only when necessary.
- 3 Order a copy of your credit report:** Order a copy from each of the three credit bureaus each year. A credit report contains information on where you live, where you work, how you pay your bills, whether you've ever been sued, arrested, or ever filed for bankruptcy, and what credit accounts have been opened in your name. Reviewing your credit report can alert you to any fraud or errors. This is very important and one of the best ways to catch identity theft. You are entitled to one free credit report annually from each of the three major credit reporting bureaus. Take advantage of it.

34567890

**4 Pay close attention to billing cycles:** If a bill does not arrive on time, it is possible that an identity thief may have taken it, so remember to check with creditors about a late bill.

**5 Guard your mail from theft:** Instead of leaving your mail to be picked up in an unlocked mailbox, take it to the post office or leave it in a post office collection box. Make sure you remove your incoming mail right away. Try not to leave mail in your mailbox overnight.

**6 Don't give out personal information** over the Internet, on the phone, or through the mail unless you have initiated contact with the receiving person or company or you are sure about the identity of the person or company. Be aware of schemes such as “phishing” in which the identity thief pretends to be from a legitimate organization or business in order to retrieve personal information from you. This might include calls or emails from someone claiming to be from your bank needing to confirm your Social Security Number or bank account number. Be aware of promotional scams that use phony offers as a way to obtain personal information.

**7 Keep your information safe online:** Only send your personal information, such as your credit card number, over a secure connection (a secure connection has an address that begins with “https” and has a small padlock at the bottom of the page. A window should

also pop up telling you that the website is secure). Make sure you have virus protection that you update regularly. Use a firewall program to protect your computer from being accessed by others, especially if you have high-speed Internet which keeps your computer connected 24 hours a day, and a secure browser. You may also want to unplug your Internet while you are not using it. Don't download any files or click on links sent to you by people you don't know.

**8 Be wary of “pharming” scams:** Pharming happens when you type in the address for a legitimate bank or e-commerce website and get rerouted to a copycat website. Identity thieves use this scam to obtain your personal information when you log into the website. Here are some ways to spot pharming:

- Login pages should be encrypted so you should see a padlock at the bottom of the browser and the address should begin with “https”. You can click on the padlock as well to make sure the site's security is registered to the right company.
- Other links on the page work.
- Highlight text. The website is a copycat if the blocks of text are actually images.
- Look for spelling or grammatical errors.
- You should never be asked to verify information.

# CONTACTS

## Ohio Attorney General's Office

[www.OhioAttorneyGeneral.gov](http://www.OhioAttorneyGeneral.gov)

For information about the Ohio Identity Theft Verification Passport Program or general questions about identity theft, please call (888) MYID-4-ME or visit the website at [www.OhioAttorneyGeneral.gov](http://www.OhioAttorneyGeneral.gov)

## Federal Trade Commission (FTC)

[www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

FTC  
Consumer Response Center  
Room 130-B  
600 Pennsylvania Avenue  
N.W. Washington, D.C., 20580  
1-877-ID-THEFT (1-877-438-4338)

## Major Credit Bureaus

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

P.O. Box 740241  
Atlanta, GA 30374-0241  
1-800-525-6285

EXPERIAN: [www.experian.com](http://www.experian.com)  
P.O. Box 9532  
Allen, TX 75013  
1-888-EXPERIAN (397-3742)

TRANSUNION: [www.transunion.com](http://www.transunion.com)  
Fraud Victim Assistance Division  
P.O. Box 6790  
Fullerton, CA 92834-6790  
1-800-680-7289

A free copy of your credit report is available from the website [www.annualcreditreport.com](http://www.annualcreditreport.com)

Or write to:  
Annual Credit Report Request Service  
P.O. Box 105283  
Atlanta, Georgia 30348-5283

Or call: 1-877-322-8228  
TDD: 1-877-730-4104

## Major Check Verification Companies

To find out if an identity thief has been passing bad checks in your name: SCAN 1-800-262-7771

To request a copy of your consumer report specifically about your checking account, contact:

Chex Systems, Inc.  
at 1-800-428-9623 or  
[www.chexhelp.com](http://www.chexhelp.com)

To request that your checks not be accepted by retailers:

Certegy, Inc. (previously Equifax Check Systems) at 1-800-437-5120

TeleCheck at 1-800-710-9898 or  
1-800-927-0188

## Social Security Administration

[www.ssa.gov](http://www.ssa.gov)

SSA Fraud Hotline  
P.O. Box 17768  
Baltimore, MD 21235  
SSA Fraud Hotline: 1-800-269-0271

## U.S. Postal Inspection Service

[www.usps.gov/websites/department/inspect](http://www.usps.gov/websites/department/inspect)

Call your local post office to find the nearest USPIS district office

If you receive notification from the Internal Revenue Service (IRS) that leads you to believe someone may have used your social security number fraudulently, please contact the IRS, Identity Protection Specialized Unit toll-free at (800) 908-4490 or via mail at Internal Revenue Service, P.O. Box 9039, Andover, MA 01810-0939





# RICHARD CORDRAY

Ohio Attorney General Richard Cordray

30 E. Broad St. 17th Fl.

Columbus, Ohio 43215

(888) 694-3463

**WE ARE HERE TO  
HELP YOU!**