**RYAN, PHILLIPS, UTRECHT & MACKINNON***
ATTORNEYS AT LAW
* Nonlawyer Partner
1133 Connecticut Avenue, N.W.
Suite 300
Washington, D.C. 20036

(202) 293-1177
Facsimile (202) 293-3411



November 1, 2006



Lawrence H. Norton, Esq.
General Counsel
Federal Election Commission
999 E Street, N.W.
Washington, D.C. 20463

Re: MUR 5815
Madrid for Congress

Dear Mr. Norton:

This response to the above-referenced complaint is filed on behalf of Patricia Madrid and Madrid for Congress, Rita Longino as treasurer (collectively "Madrid for Congress").

The New Mexico Republicans filed this complaint purely for publicity and political gain as a competitive election approaches, and should be dismissed immediately by the Federal Election Commission ("Commission" or "FEC") for the reasons set forth below.

While the complaint is somewhat unclear and inconsistent, it appears to argue that certain official state of New Mexico fliers mailed by Attorney General Madrid's state agency were somehow related to her federal campaign. As the leading law enforcement official in New Mexico, the Attorney General's office compiled information into certain guides and booklets on the topics of online sexual exploitation of children, identity theft, the high cost of prescription drugs, and the dangers of methamphetamine laboratories. Each flier referenced in the complaint alerts the public to the threats these issues pose, and provides details on how to report illegal activity or obtain more information from the Attorney General's office. These informational mailings to the people of New Mexico are clearly within the Attorney General's responsibilities and obligations to the state and have no relation to her federal campaign.

1. **The Informational Brochures Are Clearly Within the Scope of Patricia Madrid's Responsibilities And Obligations As The Attorney General of New Mexico.**

As the leading law enforcement official in New Mexico, Attorney General Madrid's duties are to take specific action in response to particular concerns for the people of New Mexico, such as creating a hotline, founding a task force, or compiling informational materials. The Attorney General mailed the fliers at issue to alert the public of the availability of such resources, and accordingly each serves a legitimate state interest.

According to the campaign manager[1] of Madrid for Congress, no member of the Madrid for Congress campaign staff requested or suggested the creation, production or distribution of these materials. Similarly, no campaign staff cooperated or consulted on any decisions regarding these mailings.

a. **Internet Predators**

In response to the growing crisis of Internet sexual predators, Attorney General Madrid developed an Internet Crimes Against Children task force, created a Cyber Safety Line,[2] and compiled an Internet Safety Guides for Parents and Teens.[3] These actions were taken in the scope of the Attorney General's responsibilities and obligations to the state of New Mexico as its chief law enforcement official. In July of 2006, the Attorney General's office mailed a brochure[4] to alert New Mexico families to the danger of these criminals, to offer families specific tools with which they may protect themselves, and to provide information on how to report the sexual exploitation of children online.

The complaint asserts that this mailing "purports to warn parents of the dangers of internet predators," and criticizes the piece as being "more about promoting Patricia Madrid's campaign for Congress than preventing sexual abuse on the Internet."[5] The complaint draws this conclusion on the basis that the flier includes the Attorney General's name and picture,[6] yet curiously excludes any mention of the task force, website, or free guides for New Mexico parents and teens.

The Attorney General's personal message within the flier clearly demonstrates the purpose of the mailing:

---

[1] *See* Attachment A.
[2] The Cyber Safety Line is a website where individual citizens may report online predatory activity.
[3] *See* Attachments B and C.
[4] *See* Attachment D.
[5] *See* Complaint at 2.
[6] *See* Complaint at 2, footnote 2: "Madrid's picture... is remarkably similar to those she displays in her campaign mailers. She seems to be wearing the same clothing, wearing the same necklace, etc." While it does appear that Patricia Madrid is wearing a black suit in the two pictures, but it is unclear and irrelevant whether they are the same suit or two similar suits. The fact that she may be wearing the same necklace is similarly immaterial.

"I need you to help me protect New Mexico's children and teens. Learn how to recognize the dangers of the Internet and how to protect your children from those dangers. Teach your teens how to protect themselves."

This brochure encourages parents and families to protect their children from pedophiles, alerts them to available state resources, and provides information on how to report predatory activity. The distribution of this information is within Patricia Madrid's duties as the Attorney General of New Mexico. This mailing does not refer to any election, expressly advocate for any candidate, nor solicit any contributions for any candidate; accordingly, it did not constitute a contribution to her Congressional campaign.

**b. Identity Theft**

After learning that the personal information of millions of veterans had been stolen, Attorney General Madrid created an Identity Theft Repair Kit.[7] This kit was created within the scope of the Attorney General's responsibilities and obligations to the state of New Mexico as its chief law enforcement official. In June of 2006, the Attorney General's office mailed a brochure[8] to provide veterans—and any other victims of identify theft—with immediate and specific steps they should take to protect themselves, as well as to inform them to the existence of the free kit.

The complaint describes this mailing as "clearly a campaign communication disguised as an official alert" and "clearly an attack...on the Federal Department of Veterans Affairs, not an appropriate subject matter for a state government informational advertisement."[9] Again, the complaint appears to draw this conclusion solely on the fact that the flier includes the Attorney General's name and picture.[10] The mailing alerts veterans to the recent and widespread theft of personal information, and offers all New Mexico residents the tools with which they may protect themselves and mitigate damages after such theft occurs. This flier falls squarely within Patricia Madrid's duties as the Attorney General of New Mexico. This mailing does not refer to any election, expressly advocate for any candidate, nor solicit any contributions for any candidate; accordingly, it did not constitute a contribution to her Congressional campaign.

**c. High Cost of Prescription Drugs**

In response to the high costs of prescription drugs, Attorney General Madrid compiled a Prescription Drug Pricing Guide in 2003 that compares the costs of medications at pharmacies around the state.[11] The Attorney General created this guide within the scope of her responsibilities and obligations to the state. In July of 2006, the Attorney General's office mailed a flier[12] to alert the people of New Mexico to the

---

[7] *See* Attachment E.
[8] *See* Attachment F.
[9] *See* Complaint at 3.
[10] *See* footnote 6.
[11] *See* Attachment G for the updated version of this guide.
[12] *See* Attachment H.

existence of an updated guide in book form, as well as to provide them with an order form.

The complaint describes the flier as "a piece of campaign literature" and incorrectly concludes that "[t]he only civic service contained in the brochure is a post card and one sentence."[13] The entire piece provides information on the free Prescription Drug Pricing Guide, and the brochure's sole purpose is to offer an order form for the updated guide. The distribution of this information is within Patricia Madrid's duties as the Attorney General of New Mexico. This mailing does not refer to any election, expressly advocate for any candidate, nor solicit any contributions for any candidate; accordingly, it did not constitute a contribution to her Congressional campaign.

**d. Methamphetamine Laboratories**

As previously stated, the New Mexico Republicans filed this complaint purely for political purposes. The clearest example of their motive may be seen in their discrepant treatment of the "Meth Labs" brochure.[14]

This flier, distributed in August of 2006, contains a message from both the Attorney General and the New Mexico Sheriffs' and Police Association. It alerts readers to the warning signs of a methamphetamine laboratory and provides telephone numbers to use to report a suspected lab. The flier contains the names and pictures of the Attorney General and the President of the Association. As with the three mailings discussed above, this flier serves a legitimate civic service and its production and distribution fall squarely within Patricia Madrid's duties as the Attorney General of New Mexico. This mailing does not refer to any election, expressly advocate for any candidate, nor solicit any contributions for any candidate; accordingly, it did not constitute a contribution to her Congressional campaign.

The complaint offers two separate and inconsistent conclusions on this flier. First, the complaint includes the Meth Labs piece in its list of four "self-aggrandizing mail-brochures," calling all four "no less than self-promotional campaign flyers, paid for by state government money, disguised as informational brochures."[15] The complaint then discusses only the fliers concerning Internet predators, identity theft and prescription drugs. As a footnote to the end of this section, the complaint concludes:

> "In 'Meth Lab' (Exhibit G [of the complaint]), produced jointly with the New Mexico Sheriffs' and Police Association – who were motivated to inform their community about the dangers of methamphetamines and clearly not interested in paying to promote Madrid's Congressional bid – the brochure correctly and appropriately lists the warning signs and health hazards posed by methamphetamine." [16]

---

[13] *See* Complaint at 3.
[14] *See* Attachment I.
[15] *See* Complaint at 2.
[16] *See* Complaint at footnote 3.

This remarkable shift in conclusions about the Meth Labs flier from page two to page three suggests that the complainants have ulterior motives: fearful of alienating the New Mexico Sheriffs' and Police Association, the complaint criticizes only those fliers that came from the Attorney General alone—despite the similarities amongst all the mailings.

All four fliers serve a legitimate public interest by alerting the people of New Mexico to a particular issue and providing information about state resources. The distribution of all four fliers was within the scope of the Attorney General's office, and did not constitute contributions to Patricia Madrid's Congressional campaign.



2. **There Is No Legal Basis For Treating The Attorney General's Official Mailings Differently From Those Made By A Member of Congress Running For Reelection.**

The entire premise of this complaint is that the Attorney General's office should not have sent any mailings while the Attorney General was a federal candidate, even if those mailings were wholly unrelated to her campaign. Such a conclusion would apply a different and more stringent standard to Attorney General Madrid than is applicable to her opponent, a current federal officeholder. Under the rules applicable to Members of Congress, they may continue to send mass mailings under the frank until 60 days before an election. Thus, Congresswoman Wilson was allowed to use the frank until September 8. The mailings attached to this complaint were all sent well before the 60 day period, and would have been permissible as official mailings if Attorney General Madrid was a Member of Congress instead of Attorney General. There is simply no legal basis for treating the Attorney General's official mailings different from those made by a Member of Congress running for re-election.

3. **The Complaint Should Be Dismissed Because It Does Not Meet The Minimum Requirements For A Complaint Under The FEC Regulations**

Attorney General Madrid and Madrid for Congress have not violated any provision of the Federal Election Campaign Act. As detailed above, all four of the Attorney General's mailings serve legitimate state interests and have no relation to Patricia Madrid's campaign for Congress. Accordingly, no state funds have been used as a source of funds for a federal campaign.[17]

---

[17] The complaint asserts that the State is a "person" under the law, and is therefore subject to the contribution provisions. However, a careful reading of the cited advisory opinions does not support that assertion. We submit that the Commission has not resolved this issue in any of the cited opinions. In Advisory Opinions 1977-32 and 1982-26, the Commission concluded that municipal corporations were corporations under the law and therefore that the law did not exempt them from the requirements pertaining to solicitations by trade associations. The analysis is based solely on 441b and the language "any corporation whatever." Neither Opinion analyzes or draws any conclusion whatsoever about whether or not States are persons. In 1999-7, issued to the Secretary of State of Minnesota, the Commission in a

Though only possible violations of the Act are within the Commission's purview, the complaint includes a wide range of accusation in its final pages that fall well beyond the jurisdiction of the Commission. This innuendo and speculation, present throughout the entire body of the complaint, is not a valid basis for a matter before the Commission.

Under the Act and Commission regulations, a complaint, to be sufficient, valid and appropriate for filing and consideration by the Commission, must conform to certain provisions set forth at 11 C.F.R. 111.4(d). Included in those minimum provisions are the following requirements:

> (2) Statements which are not based upon personal knowledge should be accompanied by an identification of the source of information which gives rise to the complainants belief in the truth of such statements;
>
> (3) The complaint should contain a clear and concise recitation of the facts which describe a violation of a statute or regulation over which the Commission has jurisdiction; and
>
> (4) The complaint should be accompanied by any documentation supporting the facts alleged if such documentation is known of, or available to, the complainant.

The complaint does not meet the low threshold set forth in the Commission's regulations for supporting a valid complaint. It appears to argue that informational mailings sent by the Attorney General are somehow contributions to her federal campaign, though the basis for this conclusion is unclear and inconsistent and no specific provision or section of the Act is cited. Merely swearing to speculative and unsubstantiated conclusions not supported by facts or personal knowledge should not give rise to Commission consideration of a matter under review.

First, the newspaper story attached to the complaint does not contain any recitation of facts that describe a violation of a statute or regulation over which the

---

footnote stated, "The Commission has not extended this exclusion [from the definition of person] to State governments or instrumentalities," when in fact none of the cited Advisory Opinions actually concluded that the State was a person. Then, in 2000-5, in an Opinion issued to the Oneida Indian nation the Commission summarized its prior opinions in another footnote by saying, "For example, the Commission has made clear that State governments and municipal corporations are persons under the Act and are subject to its contribution provisions," citing AOs 1999-32, 1982-26 and 1977-32. None of the cited advisory opinions actually made that clear. The re-characterization of the findings of these advisory opinions in footnotes in later advisory opinions does not represent a full analysis and ruling on this issue by the Commission.

While States are not specifically excluded from the definition of "person," it is also true that there is a separate definition of State in the law (2 USC §431(12)) which makes no reference to a State as a person. Should the Commission directly address this issue, there is actually no support in the definitions of the Act that states are persons for the purposes of making contributions.

Commission has jurisdiction. A discussion of an individual's contribution to a dormant political committee has no relation to the informational fliers at issue in the complaint and does not address any possible violation of a statute under the Commission's jurisdiction.

Second, as detailed above, all of the Attorney General's brochures serve a legitimate civic function and do not further Patricia Madrid's Congressional campaign. The fliers address the issues of the sexual exploitation of minors over the Internet, the theft of personal information from veterans, the high cost of prescription medications and the dangers of methamphetamine laboratories. Each provides information on how the reader may receive free information directly from the state or supplies contact information for reporting illegal activity. The fliers do not reference an election or solicit contributions, and do not contain express advocacy for or against any candidate.

Third, the inconsistencies within the discussions and conclusions reveal the political motivations of the complainants. All four mailers contain equally significant civic messages, as well as the name of the Attorney General and her picture, yet the complaint singles out one flier as acceptable (though earlier calling it "self-aggrandizing"[18]) and all others as unacceptable, without providing any additional facts or analysis to support such conclusions.

In sum, the complaint and the documents attached to it do not support a single violation of the Act. For this reason, the Commission should dismiss it immediately.

## Conclusion

For the foregoing reasons, the Commission should immediately dismiss this complaint.

Respectfully submitted,

Karen Zeglis

Lyn Utrecht
Eric Kleinfeld
Karen Zeglis

[18] *See* Complaint at 2.

# ATTACHMENT A

**BEFORE THE FEDERAL ELECTION COMMISSION**

| | |
|---|---|
| **In re MUR 5815, Madrid for Congress** | ) |

**DECLARATION OF CAROLINE BUERKLE**

*I, Caroline Buerkle, do hereby certify:*

1. I am the campaign manager of Madrid for Congress, registered with the Federal Election Commission, Id. No. C00415885.

2. Neither I nor any member of the Madrid for Congress campaign staff participated in the creation, production, or distribution of any mailings that may have been sent from the Attorney General's office.

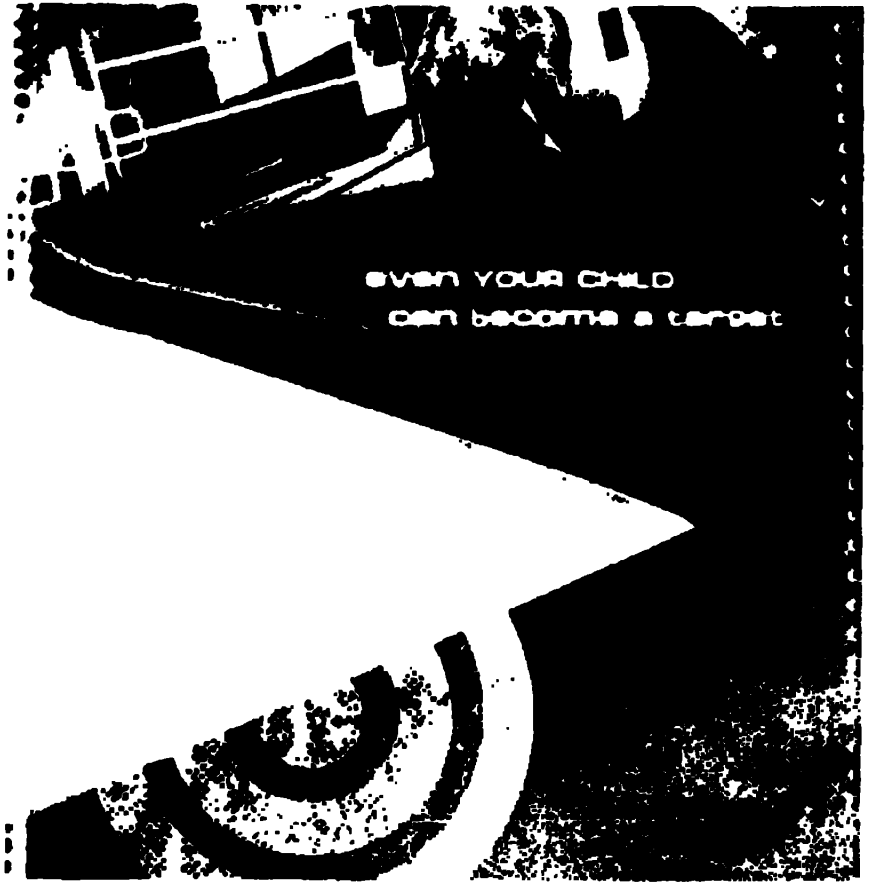
3. Any mailing sent from the Attorney General's office was not made in cooperation, consultation or concert with Madrid for Congress, nor were they sent at the request or suggestion of any staff member of Madrid for Congress.

I declare under penalty of perjury that this declaration is true and correct.

Signed: Caroline Buerkle
Caroline Buerkle

Date: 11-1-04

# ATTACHMENT B




Dear Parents,

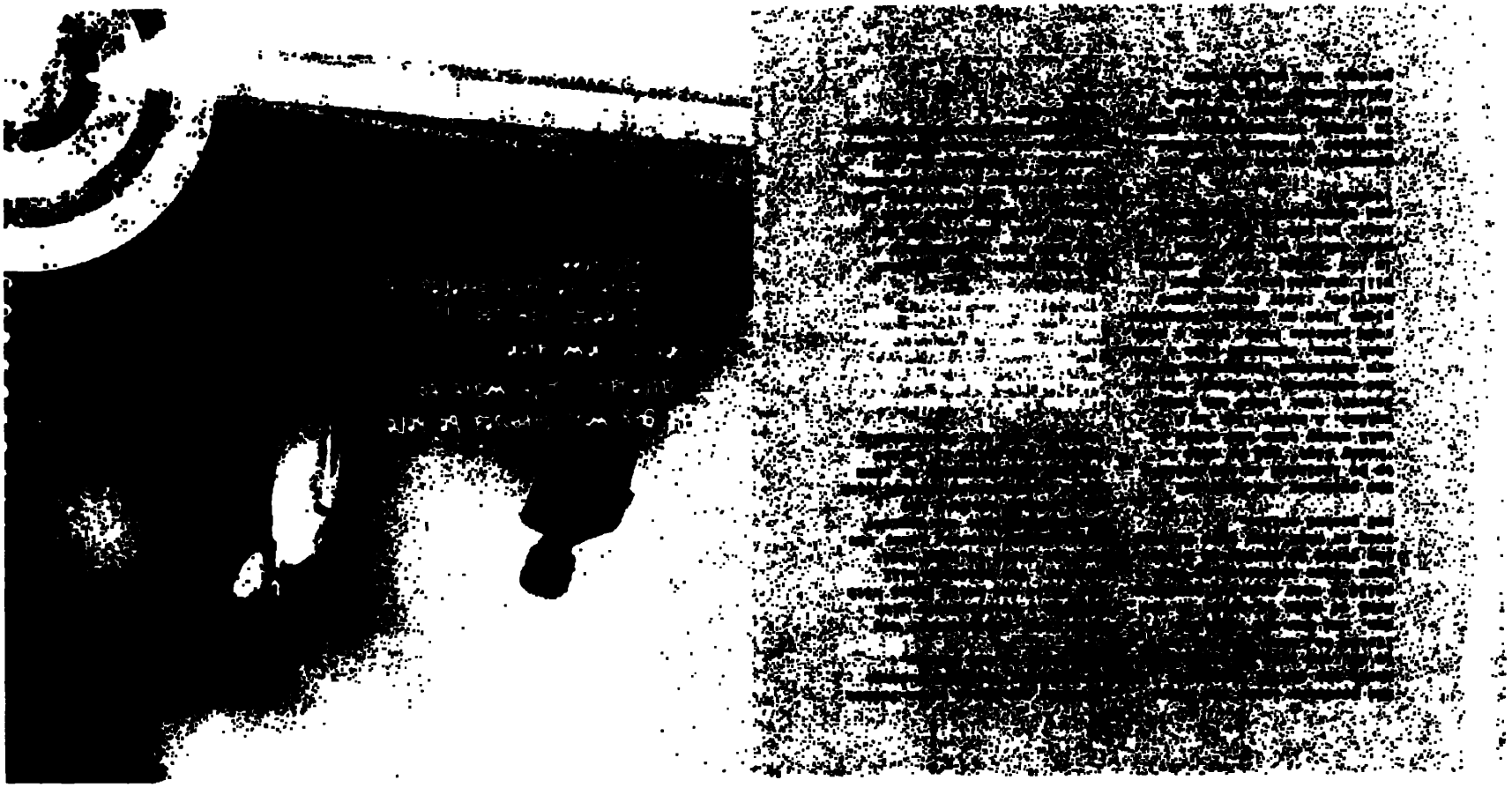
[illegible]

[illegible]

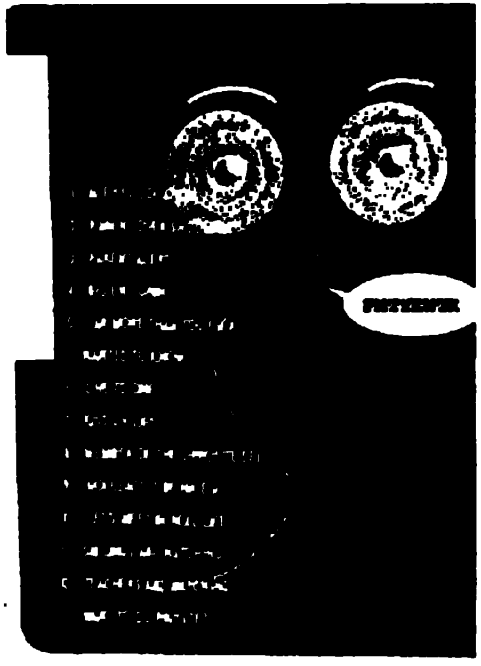
[illegible]

This [illegible] I urge you to review this booklet cover to cover. Half is targeted specifically for the teenage audience but may be appropriate for younger children, as well. The Justice Department survey of youths ages 10 to 17 tells us that one in five children have received a sexual solicitation while on the Internet and only one quarter of those children chose to tell their parents about it. [illegible] I hope this booklet will help.

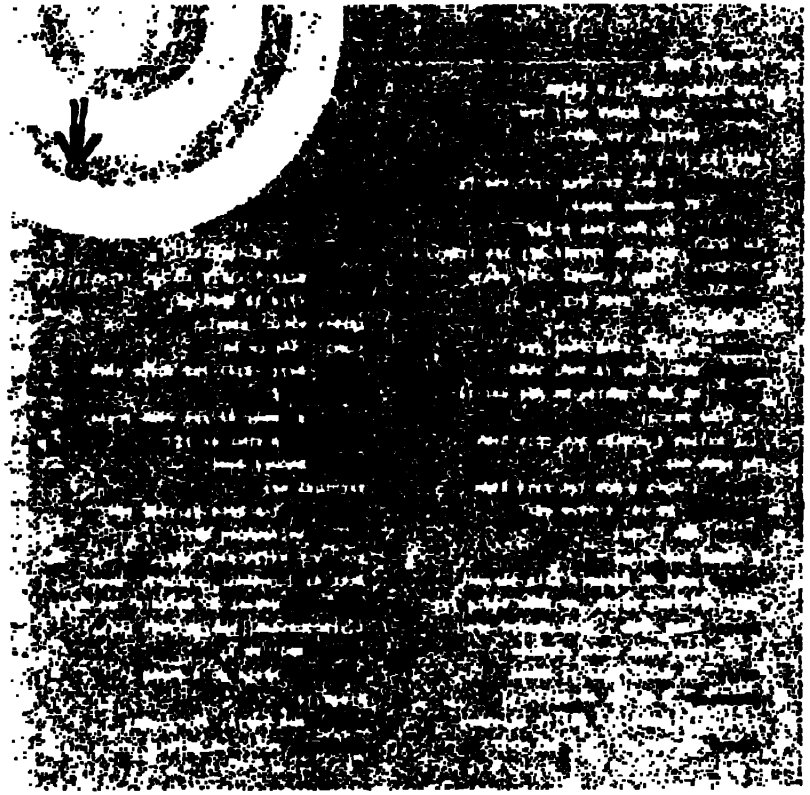
Patricia Madrid
New Mexico Attorney General

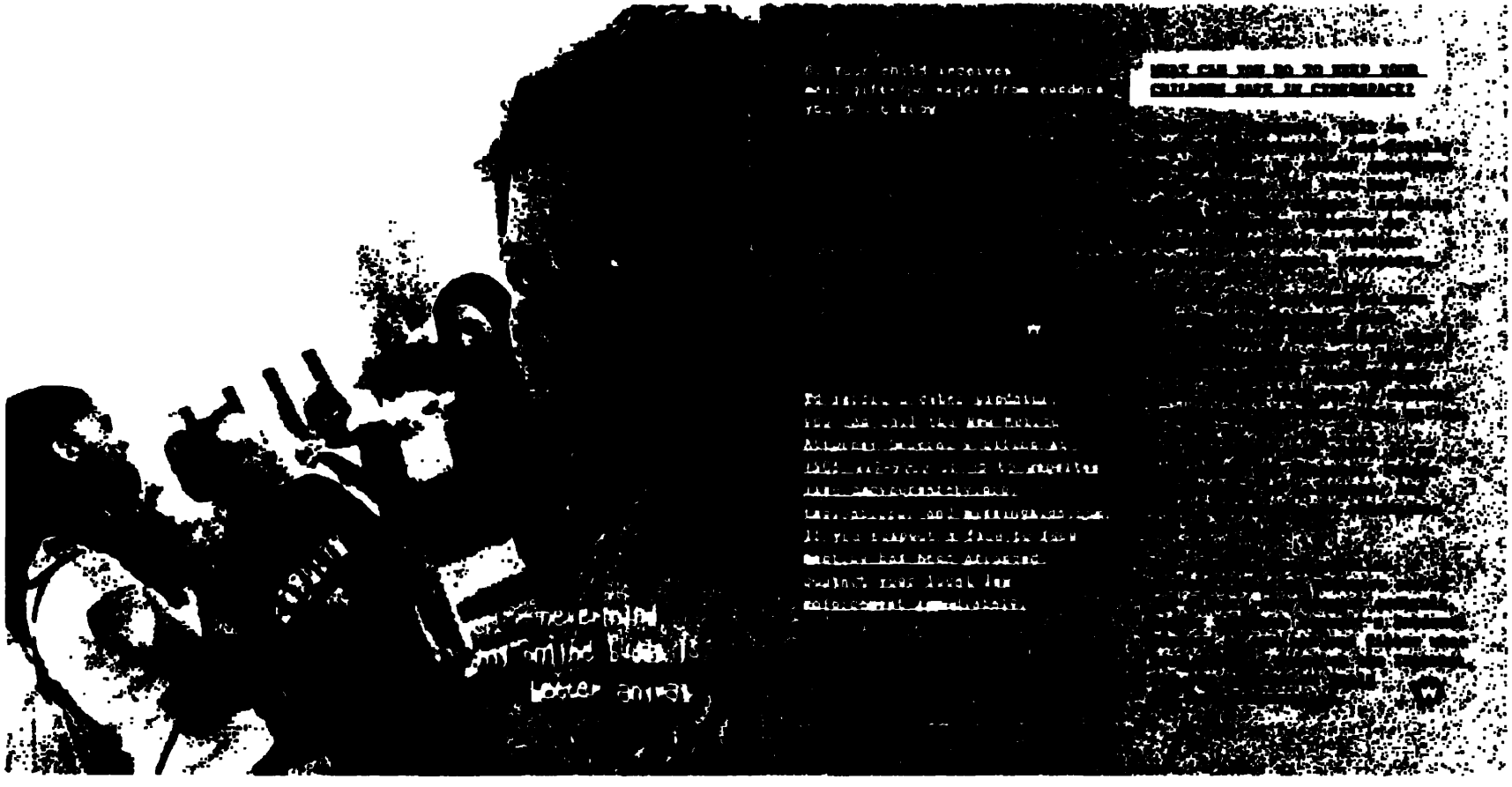



1. ASL
2. POS
3. PRI
4. BRO
5. PNTTSBRTK
6. 121
7. KOL
8. NOTOS
9. WINGK
10. LNDRL
11. SAW
12. TAW
13. WTOP




Don't feel bad if you don't.
A national survey showed that only between 4 and 8 percent of adults could correctly identify the acronyms.





## WHAT CAN YOU DO TO HELP YOUR CHILDREN SURF THE CYBERSPACE?

**ONLINE ACTIVITIES and their POTENTIAL CONSEQUENCES:**

### 1. Filling out online profiles

Filling out profiles will allow predators to see personal information about your child, such as their real name, phone number, address, school name, etc. and will allow the predator to "find" your child in real life.

### 2. Downloading pictures or using screen names

Downloading a picture may bring hidden viruses, which may destroy your computer, or place "cookies" that allow the sender to track where you or your child goes on the Internet, as well as key stroke trackers that may be used to steal your child's identity.

### 3. Responding to offensive or threatening messages

These messages are often posted by the author simply to get a reaction from people to see who will respond and to get a conversation going.

### 4. Posting pictures on the internet

In addition to allowing anyone to get a look at your child, digital photo manipulation could put your child's face on another body, which could be spread all over the Internet, or your child could be black-mailed into sending more photos.

### 5. Posting personal profile information

Because these popular online features are virtual diaries, they give online predators a more intimate look into your child's thoughts and feelings. By reading postings on a blog, a predator can get a greater insight into a child's vulnerabilities, likes and dislikes and can "tailor" his message to target the child. Even though this may take longer for the predator to learn about the child, the posting of the child's thoughts and feelings give the predator more information than even an online profile.

### 6. Chatting with strangers in a chat room

It's easy to lie online because a person's identity can be easily disguised, so seemingly innocent conversations can easily have harmful ulterior motives. Don't believe everything someone tells you in a chat room.

### 7. Being a webcam

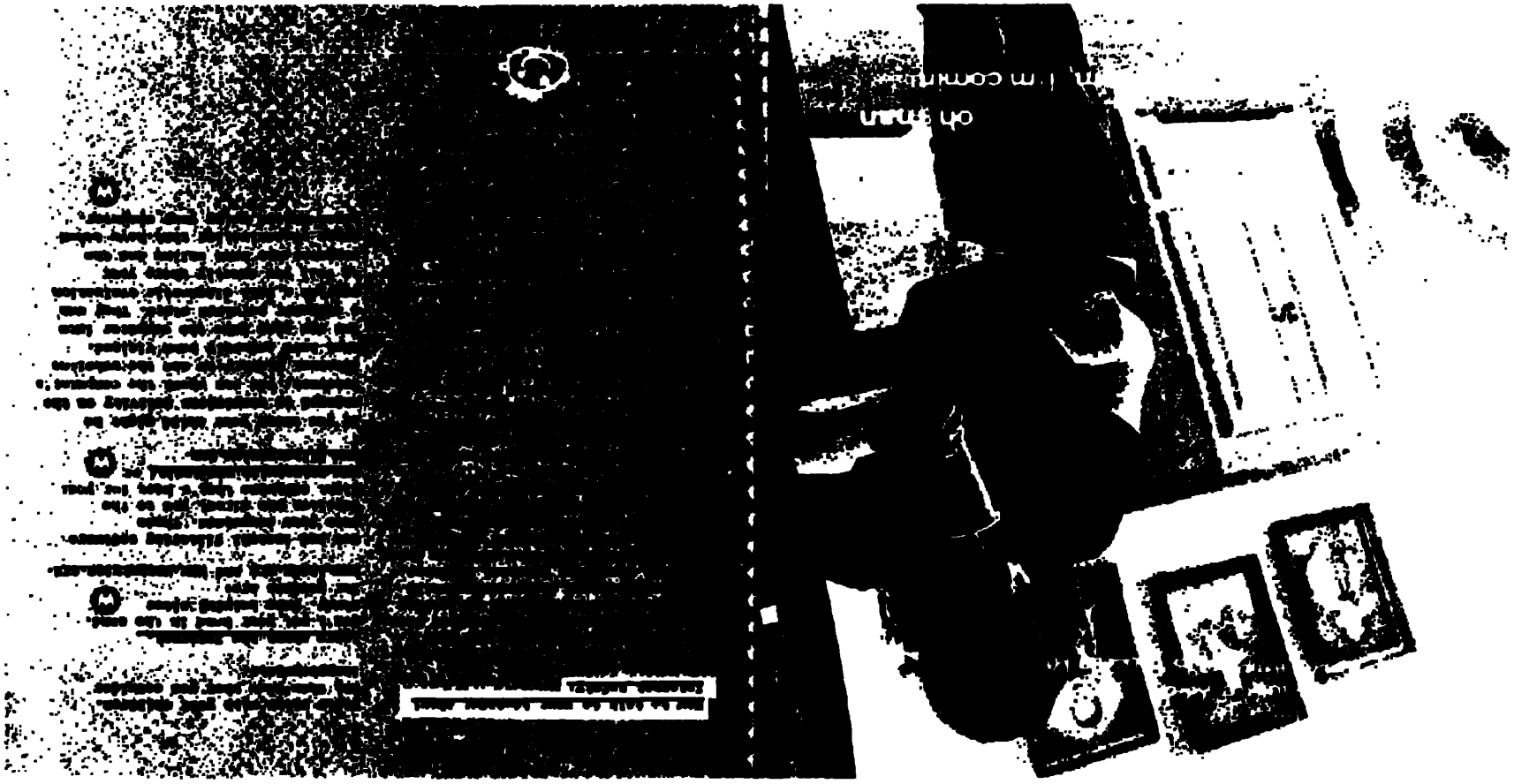
For a predator, a webcam is the next best thing to an in-person meeting. By allowing people to view a webcam, your child is essentially opening the shades to your home or his/her bedroom and allowing a complete stranger to watch them through that window. Predators will use what they see to take advantage of your child. They may record the video you send and post it for the world to see or simply wait and use it against your child later.

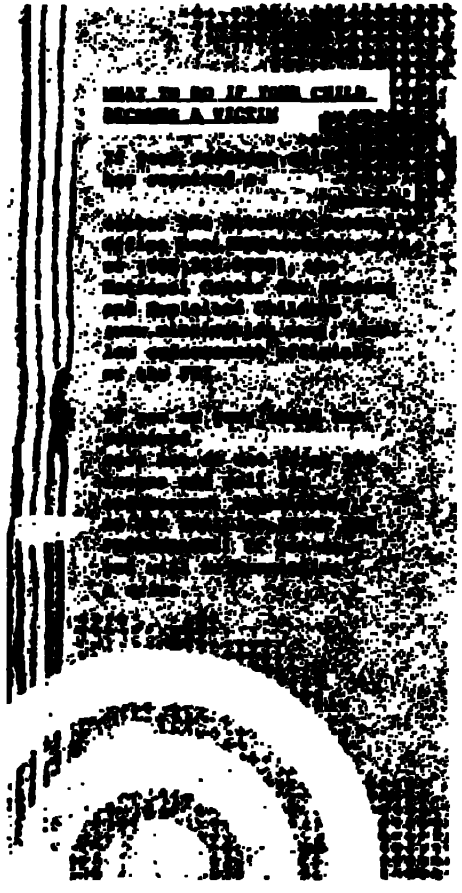

### 8. Accepting an invitation to view live webcam from strangers

By accepting an invitation to view live webcam from strangers, your child could be exposed to nudity and sexually explicit material which could be disturbing. Ask your child to never accept an invitation to view a webcam or click on a link in a chat room.

### 9. Allowing a live webcam with someone you don't know

Your child could be hurt, molested, raped, kidnapped or worse during a face-to-face encounter.





## WHAT TO DO IF YOUR CHILD BECOMES A VICTIM

[illegible]

## INTERNET SAFETY TOOLS FOR PARENTS

There are a number of different tools parents can use to protect their children from the dangers of the Internet. Although none of them are 100% proof, they can help. Here are a few:

- Computer Placement
- User Profiles
- Web Browser Controls
- Viewing Internet History
- Filtering/Blocking/Monitoring Software
- Filtered ISPs

### Computer Placement

Keep the computer in a common area of your home. It's easier to monitor what your children are doing without having to pry if the computer is in an open area of your home, such as a living room, a loft, or the kitchen. Don't place the computer in a room where your child can close the door and go online.

### User Profiles

Newer versions of Windows and Apple's OS allow for multiple user profiles to be set up. Every person who uses a the computer can have their own user name and password. In order to gain access to the computer, the user name and password are required. This allows for different levels of access to be setup for each of the different users and also makes it easier to track and find out what each of the different users are doing on the computer. To get more information about setting up user profiles, consult your computer's help files.

### Web Browser Controls

Most web browsers have a way to filter and block inappropriate websites from being accessed. Web browser settings can be used in conjunction with user profiles to fine tune the level of access different users have to the Internet. By fine tuning these controls, you can customize the types of content that each user can gain access to. To get more information on using these settings, consult your browser's help files.

### Viewing/Deleting Internet History and Temporary Internet Files

In order to track your child's online activity, you can use the Internet History and Temporary Internet Files to see what websites have been accessed recently. More savvy computer users can easily delete this information from easy access, but this information is still typically accessible by a computer expert. For more information about viewing Internet History and temporary Internet files, consult your browser's help files.

### Filtering

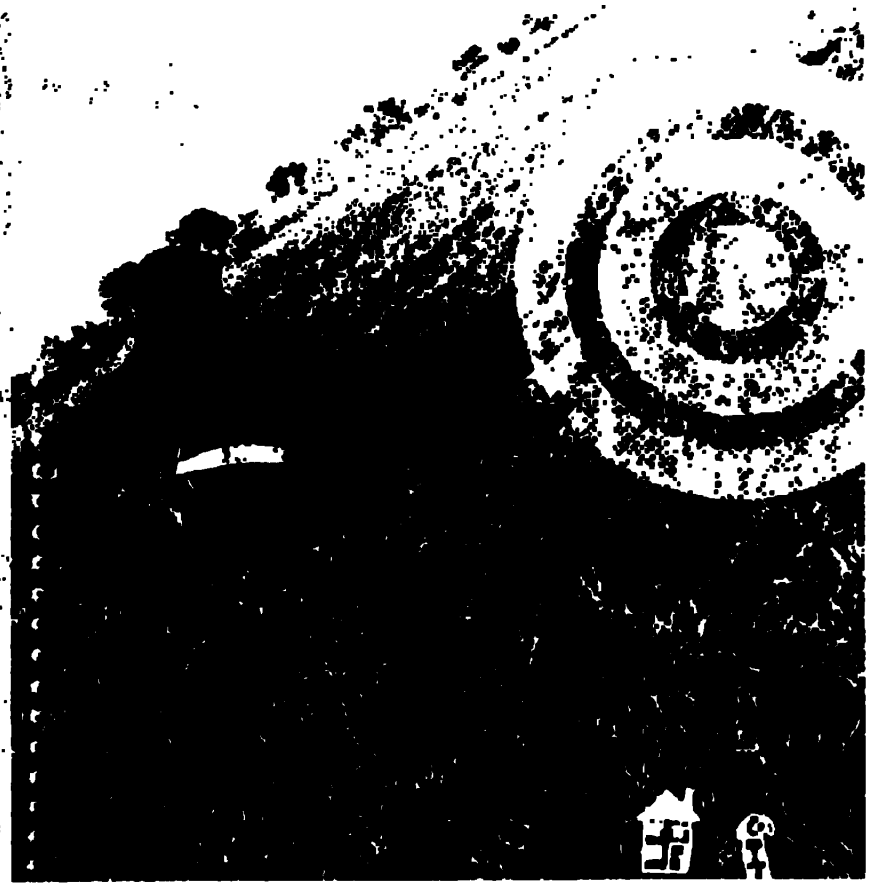
There are many different software programs available for purchase that help make the Internet safer for your children. Some of the options these programs can give you are:

- Blocking chat rooms and/or instant messaging
- Blocking downloads
- Disabling links in chat rooms

- Allowing only approved addresses to email your child
- Filtering websites
- Filtering pornography or allowing your child to use child-safe search engines
- Recording instant message conversations or chat room conversations
- Notifying you when your child tries to access an inappropriate website
- Limiting the time your child spends online
- Operates in the background without your child's knowledge
- Allowing third-party rating of websites
- Recording every key stroke your child makes
- Recording and sending you pictures of your child's computer screen as they are using it

Not all of these options are included in each software program. Each program is different. Compare some of these programs and find which one suits your needs.

Most Internet Service Providers, such as AOL, Comcast, MSN and Qwest may also be able to provide you with some filtering and blocking tools to help protect your child online. Contact them for more information.



# ATTACHMENT C

Dear Teen,

You may not think I can tell you much about the Internet that you don't already know, and that might be true. But do you know enough to keep your not-so-nice friends and younger siblings safe while online? Have you told them that a chat room that attracts them also attracts predators that are looking for younger victims? Have you told them how to identify a cyber predator? Have you warned them that giving away personal information can lead a predator to their school or home?

There are predators out there who are looking for young people and what they have in mind is not only dangerous, it can be deadly. The real problem is that it isn't always easy to spot a predator. Predators are very good at pretending to be nice and understanding friends. A predator is likely to sound like the generous and comforting friend that anyone would trust. And that is exactly what they want because trusting a predator can lead a young person to do any number of things that he or she will regret.

I hope this booklet will help you help your friends and siblings to be safe online.

Patricia Madrid
New Mexico Attorney General

## WHAT'S THE PROBLEM?

The Internet can be a really great tool, fun to surf in your spare time, and totally entertaining. But sometimes, some things are too good to be true.

Unfortunately, we live in a world where people sometimes take advantage of others, especially youth. It's good to be prepared: this may happen to a friend or a sibling. Anything on the Internet, whether it's chat rooms or web sites, that attracts you and your friends will also attract predators.

>>> Good ca.

Many predators, people searching for young adults and teens to rape, kidnap or harm, now use the Internet as their tool of choice. Instead of doing research, like you are doing for that English paper, a predator uses the Internet to find victims. Predators manipulate things that teens are interested in, messaging meeting to form relationships with young people. They seek the trust of young people. When a trust forms, they ask to meet somewhere to check out a movie, window shop or get something to eat. Typically, a predator does all this while posing as a young adult or teenager himself.

Who are the cyber predators? Not who you think:

>> 99% are male

>> Above average intelligence

>> Above average income

>> Have a successful career

>> 91% are Hispanic white

>> Have computer knowledge

>> Many have children of their own

>> Have no criminal history related to sex crimes

>> 84% are older than 25

## HOW THEY LURE YOUNG PEOPLE:

[illegible] They look for many clues to figure out what you like, who you are and sometimes, even where you live [illegible] [illegible] by young people.

## [illegible] / SCREEN NAMES

[illegible] gold-star [illegible] your pager or [illegible] screen name. But by doing so, what information have you given [illegible]?

This tells the hacker that you like to chat, [illegible] and that you were born in 1983.

This tells the hacker that you are [illegible] Jeffrey Dahmer fan, you [illegible] like the [illegible], and you are likely 14.

Armed with this information, a hacker will talk to [illegible] your shopping and [illegible] this politics to [illegible] about [illegible], pager and music.

It may not seem important, but providing a predator with any information that helps him [illegible] how to become a trusted friend is unnecessary risk potentially dangerous.

WHEN CHOOSING A NEW NAME OR SCREEN NAME, think of the game "Mad Lib." [illegible] of the following [illegible] to select a new name:

>>> Adjective + noun
[illegible]

>>> Size + animal
[illegible]

>>> Noun + noun
[illegible]

>>> Random number + ice cream flavor
[illegible]

>>> Actor's name + action verb
[illegible]

>>> Color + foreign food
[illegible]

A user name or screen name with a random selection of words such as "Soupchow" is much better than a potentially descriptive identifier such as "Kissyfish". Make sure your name identifier doesn't relate to you, your age, your school, your location, or your interests.



**2/ PROFILES.**

Profiles can provide predators with a lot of useful information. Profiles ask for information like your real name, birthday, address, phone number, hobbies and what school you go to. Filling out this information is meant to be useful to other teens and young adults who are looking for people to meet with who are interested in the same things. The problem is that predators use personal information to gain your trust and find ways to manipulate you. Filling out profiles is not required to use most chat programs, and filling them out is a pain in the back anyway. To protect yourself, fill out profiles only on sites that allow you to control who has access to the profile.

**3/ WHAT YOU SEE.**

Some predators will do something called "spamming" (send you, like, a lot of messages). A predator will go to a room of young adult chat rooms and pick a nice name to follow through that room. The predator will slowly accumulate information about that user by simply reading what they are chatting about with other chatters. Using abbreviations and terms such as parents, parents, friends and other family members. The terms seem like the perfect place to pick up on [illegible] people who are discussing your life. Be watch out for people who continue to [illegible]. Often, predators will play on your emotions by saying they went through the same thing.

**4/ SELLING STUFF:**

By selling things online, you can always make a quick buck off of the old fashioned [illegible]. Many Facebook [illegible] you put in your birthday when you were six. But selling things can also provide dangerous information to predators. Sometimes, a seller will provide their telephone number so that people interested in purchasing can call and ask questions about the item they [illegible] that's always well. Instead of use your telephone number to trash you down. Providing your phone number not only [illegible] a potential stalker where you live in, it also can lead them to your house.

**THEIR TECHNIQUES:**

Identifying a cyber predator is difficult because they sound like anyone else. [illegible] way. Predators have many techniques that they use to convince you that they are just like you, can relate to your problems, and would like to become your real friend instead of your online buddy.

**Sending you special stuff:**

[illegible] may not want to see [illegible]. When an online buddy sends you sexually explicit material, whether you want it or not, it is smart to stop speaking to that buddy. Predators use this technique to [illegible] or befriend you. Almost all of the time this material is unwanted, but if you continue to speak to this person, they will push you to do more things than just look at inappropriate material. [illegible] online buddy any longer.

**Pretending:**

As stated in the previous section, predators will often disguise themselves as teenagers and young adults. [illegible] These people can be very convincing and, without realizing what you have done, you may befriend a predator. [illegible] is your same age and who is an adult, but being safe means ending communication with any online buddy if they begin to harass you. Remember, never give out too much personal information (not even an email address) and if anything mean or inappropriate happens, don't be afraid to tell your parents.

**Threats:**

If an online buddy begins to threaten you because you refuse to meet him or speak to him anymore, the best thing to do is tell your parents. Predators exploit any weaknesses they can find. A predator's objective is to make you do what he wants whether or not you want to do it. [illegible]

**How predators manipulate**

Gaining access to your room or reading your blogs (online journals) are easy ways for a predator to learn how to talk to you and earn your trust. By following you through that room, a predator can gather information about you and make you feel comfortable enough to talk to them about anything, even revealing secrets. Because all someone who knows everything about conversations you have been having or are quick to say "the same thing happened to me."

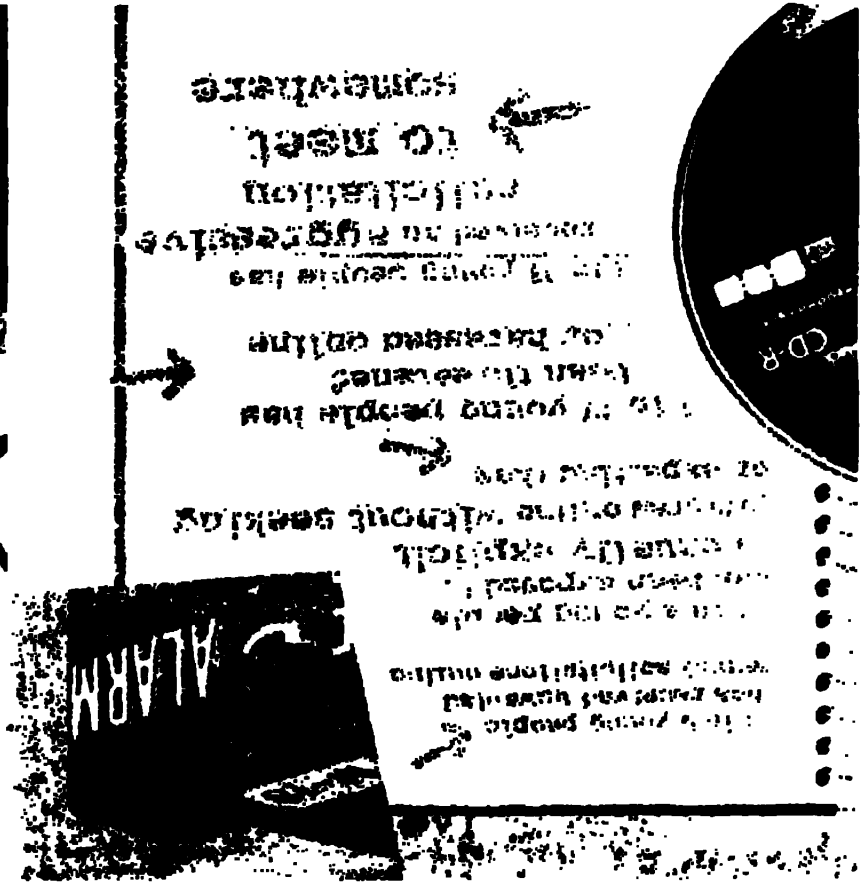
**Photographs**

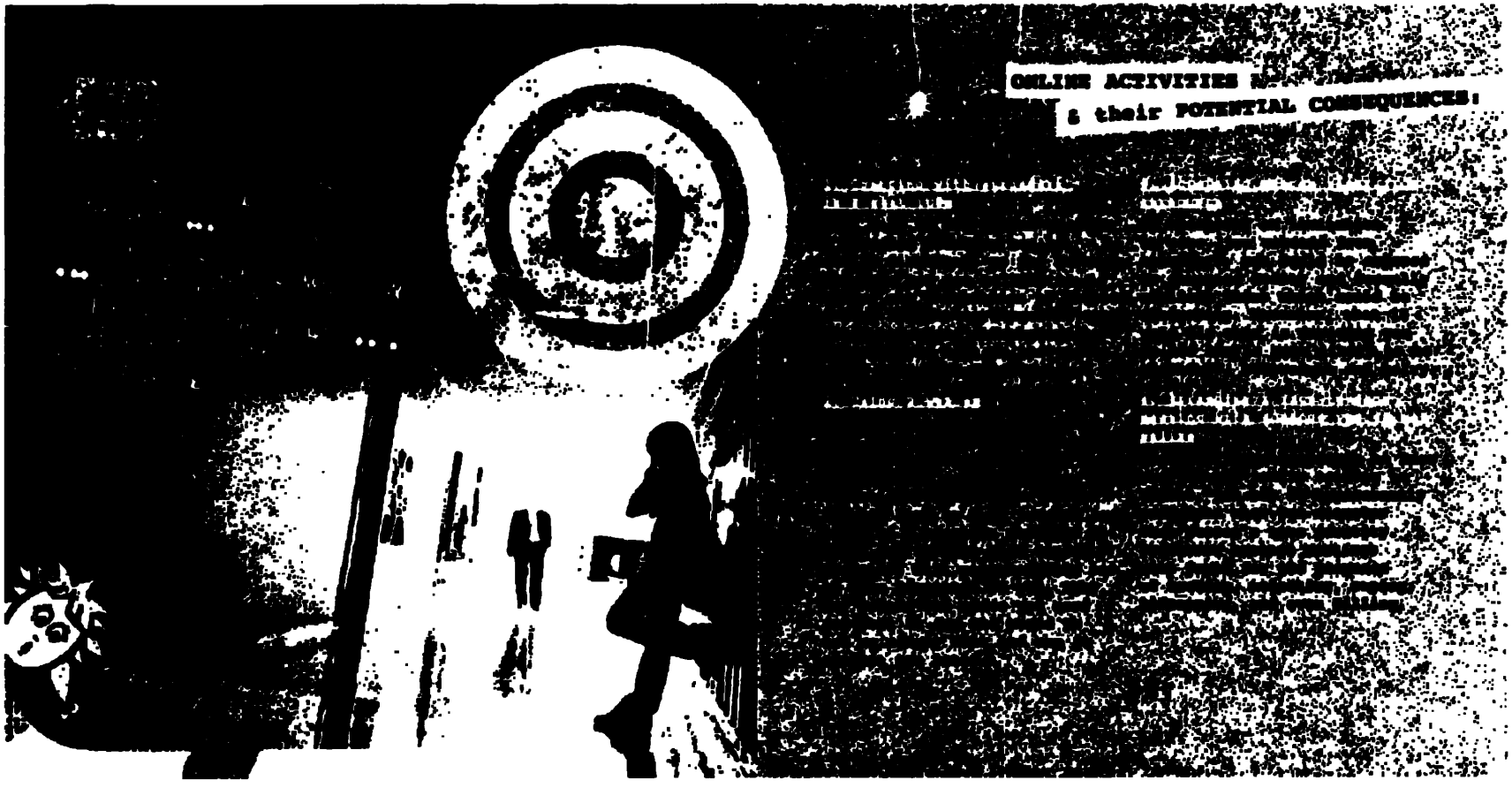
Posting photographs online is becoming more and more popular, especially with that teens, blogs, and online social networks like "myspace.com." Unfortunately, there are a number of reasons why photographs are a problem:

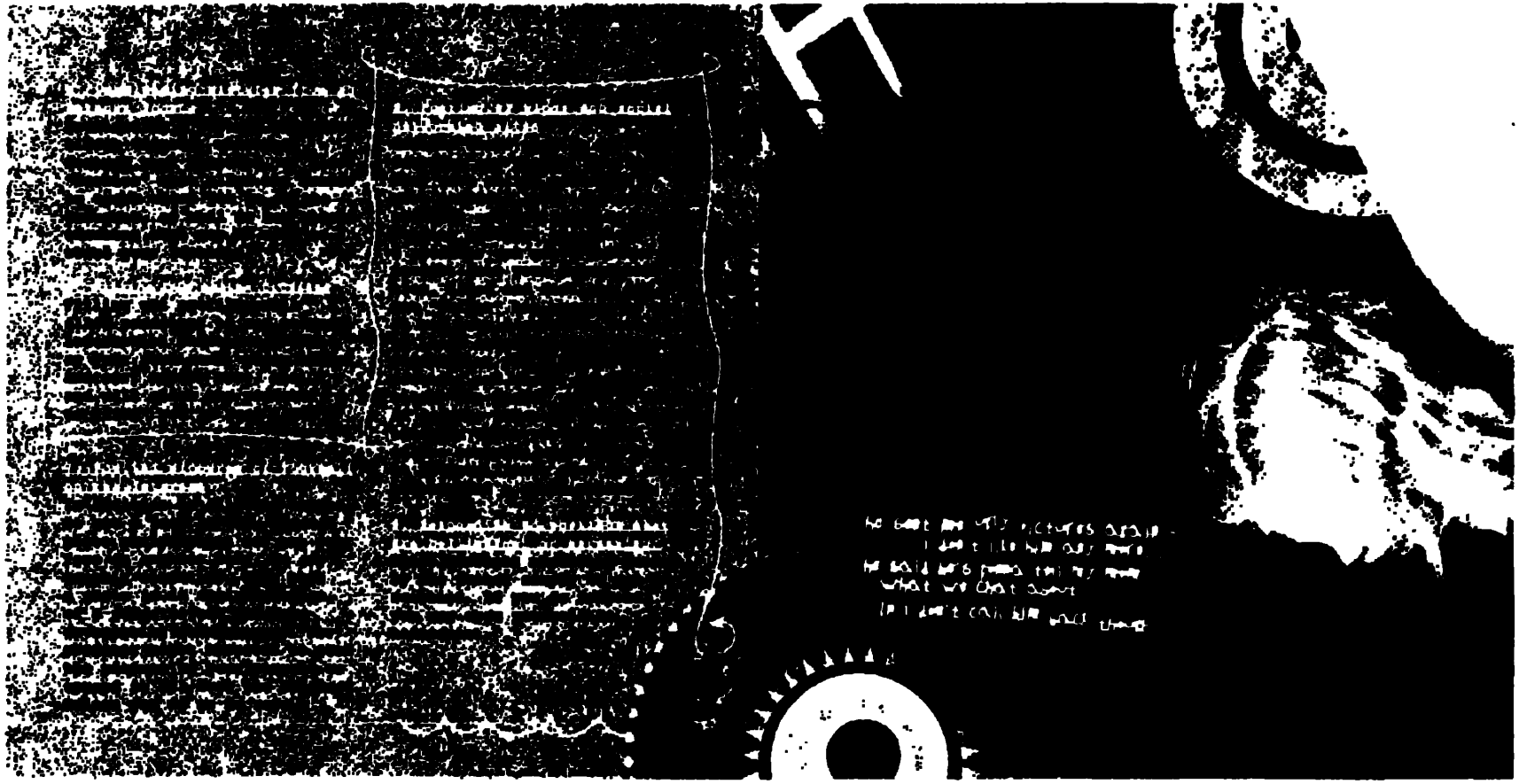
- Combining a photograph with personal information can make it extremely easy for a predator to find his way to your school or doorstep.
- Photographs can be manipulated—your face put onto another person's body in a sexually explicit photograph—and passed for anyone, including your parents, to see.
- It is important to understand that a predator wants a picture of his prey. He will ask for a photo, he may ask for you to pose partially or completely undressed. If you send a predator a picture of yourself that you would not want your parents or friends to see, the predator can use that photograph to blackmail you into sending more. A predator is trying to control the person so he is feeling so. This is not a relationship about love; it is about control.
- Pictures may be fun, but make sure that you post pictures only in places where people you know can view them. Be very careful when posting your photo online.

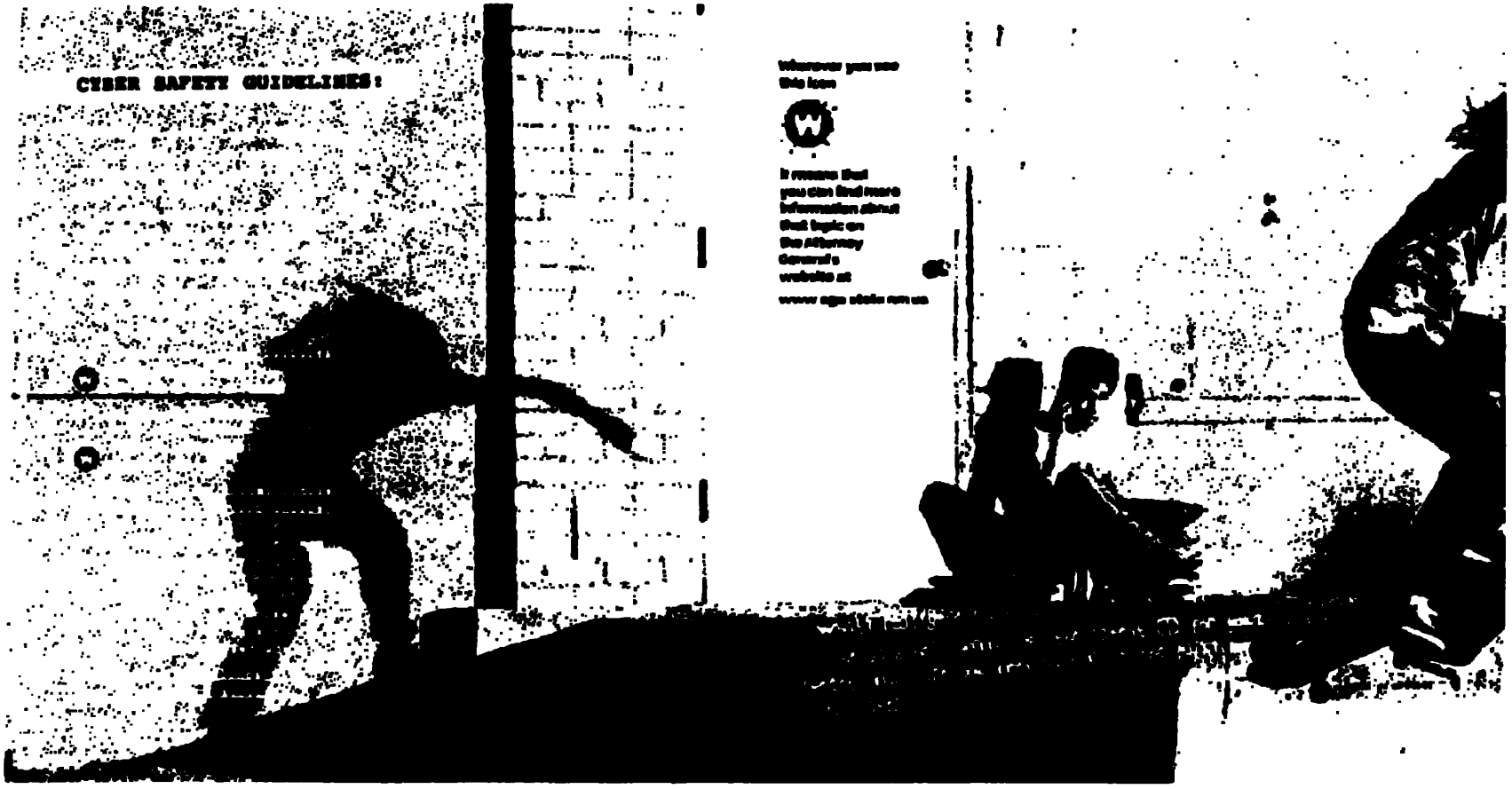
**Email**

Sometimes you meet people who you really like online and you want to talk to them more than just in chat rooms. Giving out your email address or instant messaging screen name can be a good way to keep your conversation private. But be careful when you give out your email address. Often times your email has a profile that can be easily accessed by a predator. Email is personal and is [illegible] than chatting [illegible]. And the people who have your email address [illegible] to friends and family. Try not to give it to people you meet in chat rooms and set your profile to not display your email address.


ALARM
CD-R






CYBER SAFETY GUIDELINES:
Wherever you see this icon
It means that you can find more information about that topic on the Attorney General's website at

# OTHER IMPORTANT INFORMATION YOU SHOULD KNOW

KEEP ON TOP OF THE LATEST SCAMS

# ATTACHMENT D

# BE AFRAID

**A true story of a New Mexico girl, just last year:**

She was just 12 years old when an online chat participant asked that she send pictures of herself. These weren't pictures of her playing sports or at a dance recital. They were pictures she had taken of herself in the nude with her own digital camera. By the time she was caught, it was too late. She had sent images of herself to more than one Internet predator.

***Who's watching your daughter?***

*Attorney General Patricia Madrid is taking*

THE ALBUQUERQUE TRIBUNE JANUARY 19, 2006

**"State Attorney General Patricia Madrid has taken a much needed, aggressive stance in combating Internet sexual predators who target children."**

# action to keep New Mexico's children safe

Every day predators are exploiting New Mexico children and teenagers online. Studies show that one of every five children has received unwanted sexual solicitations online.

**New Mexico Attorney General Patricia Madrid is taking aggressive action to stop these predators from hurting our children:**

- Cyber predators, child pornographers, and criminals who exploit children are being found and arrested by Attorney General Madrid's Internet Crimes Against Children (ICAC) task force.
- Attorney General Madrid also created the New Mexico Cyber Safety Line—a website where anyone can report online sexual exploitation of a minor. It can be found at www.NMCyberSafety.org.
- Attorney General Madrid's Internet Crimes Against Children task force investigates reports received on the New Mexico Cyber Safety Line and patrols the Internet looking for online predators.

## *Attorney General Patricia Madrid needs your help to protect New Mexico's children from online predators.*

**Download or request a free copy of NM Attorney General Patricia Madrid's *Internet Safety Guide for Parents and Teens* at www.ago.state.nm.us or call 1-505-222-9000.**

New Mexico Attorney General's Office
111 Lomas Blvd., NW, Suite 300
Albuquerque, NM 87102





"I need you to help me protect New Mexico's children and teens. Learn how to recognize the dangers of the Internet and how to protect your children from those dangers. Teach your teens how to protect themselves."

# Patricia Madrid

**Download or request a free copy of NM Attorney General Patricia Madrid's *Internet Safety Guide for Parents and Teens* at www.ago.state.nm.us or call 1-505-222-9000.**

**Report suspected online predators to www.NMCyberSafety.org or call 1-505-222-9000.**

# ATTACHMENT E

28044222344


NEW MEXICO ATTORNEY GENERAL'S OFFICE www.ago.state.nm.us

Albuquerque 505.222.9000 Santa Fe 505.827.6000


WE ARE HERE TO HELP YOU!


NM Attorney General's Office
111 Lomas NW, Ste 300
Albuquerque, NM 87102



# IDENTITY THEFT REPAIR KIT

SUBJECT:
Identity Theft

BROUGHT TO YOU BY:
New Mexico Attorney General
Patricia Madrid

WARNING: fastest growing white-collar crime in the US

## Message from Attorney General
## Patricia Madrid

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.

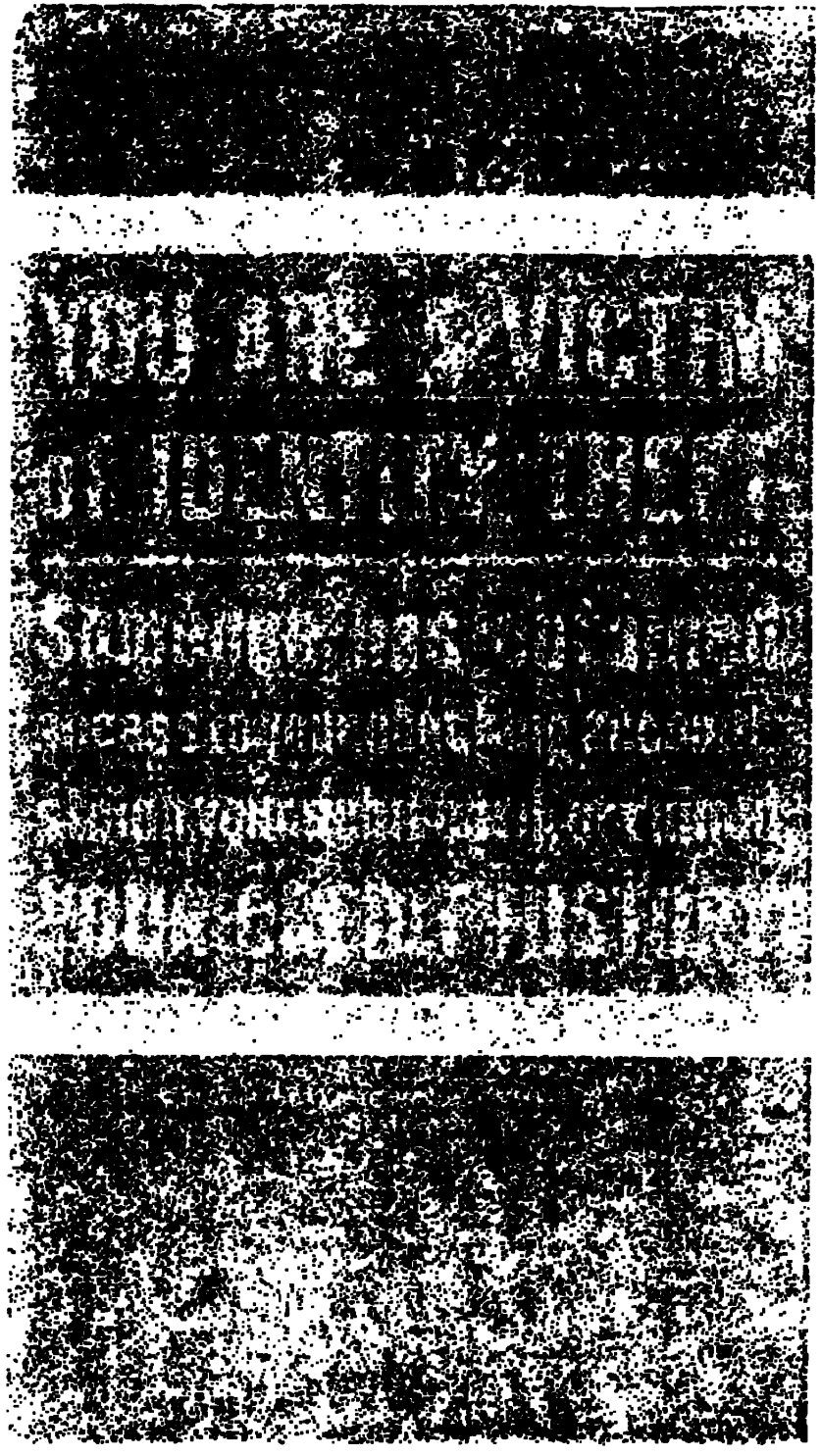
The effects of identity theft can be devastating. It is vital for you to take action to correct the damage. Use this handbook to guide you through the steps of repairing the damage done by identity theft and preventing identity theft from happening in the future.

Patricia A. Madrid

## Table of Contents








# 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 your 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 identifying 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 or Internet.

## 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, 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.





# 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 3 page 16). If you close an existing bank account and open a new one, be sure to create new PINs (Personal Identification Numbers) and passwords.

## STEP 3: FRAUD ALERT

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 |
| --- | --- |
| Lasts at least 90 days. | In your file for 7 years. |
| 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. | 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. |

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.

[redacted]

**EQUIFAX**
www.equifax.com

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

**EXPERIAN**
www.experian.com

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

**TRANSUNION**
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.

FRAUD ALERT






## STEP 4:
## 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 P4 for contact information on these organizations.*

| | | |
|---|---|---|
| You find any accounts tampered with or opened without your knowledge | 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 |
| Your ATM card, credit cards, or checks were stolen | 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 |
| You find inquiries on your credit report that you did not know about | 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 |
| You find inaccurate information on your credit report | By phone and then in writing, notify the three major credit bureaus and request the information be corrected. | Credit Bureaus |

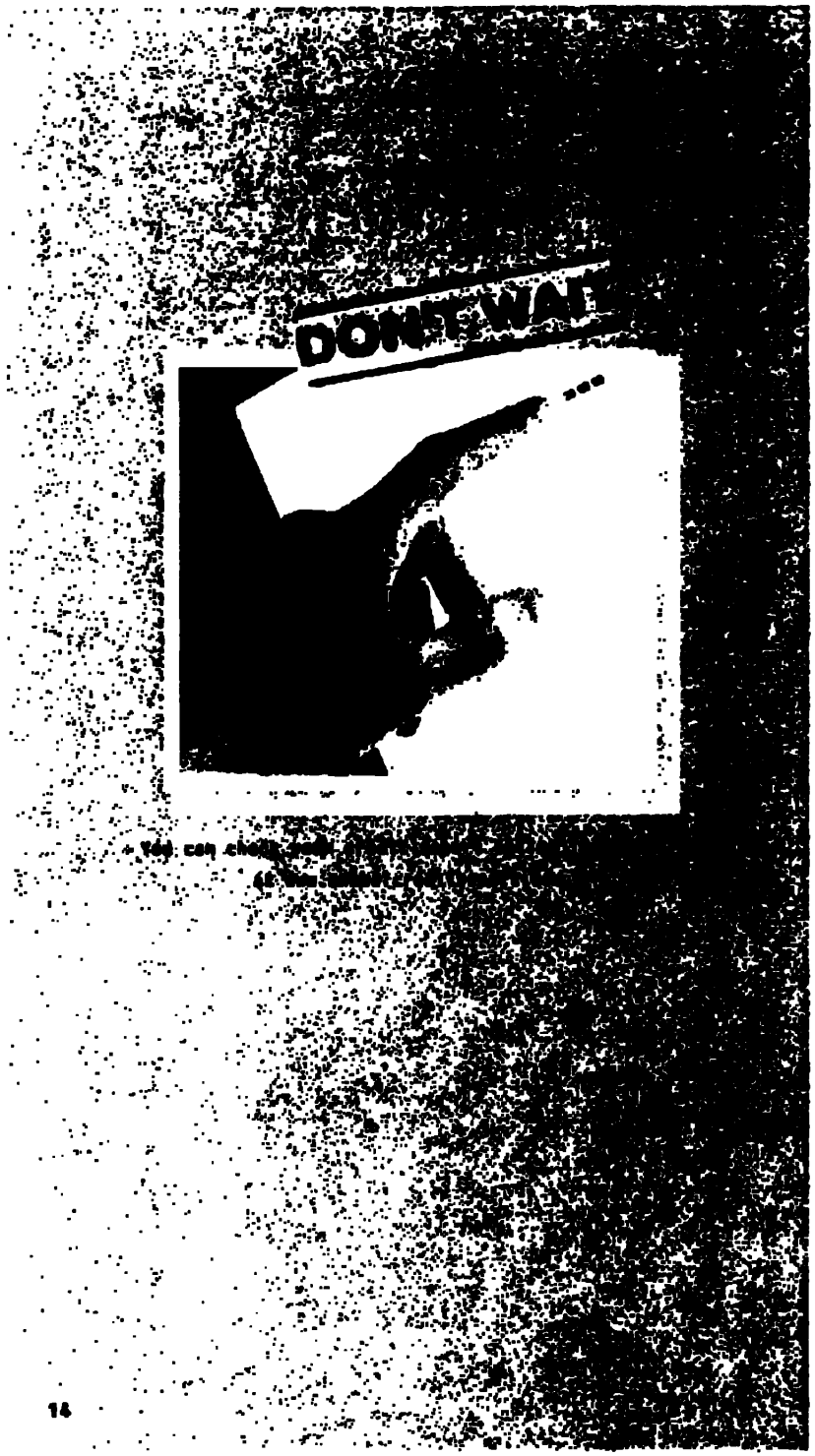
*Cont. on next page*

*Step 4: Fixing Specific Problems cont.*

| | | |
|---|---|---|
| You have reason to believe your Social Security Number (SSN) has been stolen or misused | 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. | Social Security Administration |
| 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 | 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. | U.S. Postal Inspection Service (USPIS) |
| You've lost your passport, it was stolen, or you believe it is being misused | Contact the United States Department of State through a field office or on their website. | United States Department of State (USDS). |
| You think your name or SSN is being used to obtain a false driver's license | Contact the Motor Vehicle Division (MVD). Make sure you don't use your SSN as your driver's license number. | Motor Vehicle Division (MVD) |
| You think an identity thief has interfered with your security investments or a brokerage account | Report it to your broker or account manager as soon as possible. File a complaint with the U.S. Securities and Exchange Commission. | Your broker/account manager, U.S. Securities and Exchange Commission |



| | | |
|---|---|---|
| A phone service provider reports that someone, perhaps your spouse, is using your calling card, or international calls are being billed to your cellular phone | Cancel your account and/or calling card. Use new PINs if you open new accounts. | Your service provider |
| A debt collector contacts you trying to collect on a loan that you did not take out | 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. | Debt collector |
| You have been wrongfully accused of having committed a crime perpetrated by someone pretending to be you | File an impersonation report, have your identity confirmed, and prove your innocence by comparing your information to that of the identity thief. | 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 Defenders' Office or the State Bar Association in order to find an attorney |
| You believe someone has filed for bankruptcy in your name | Write to the U.S. Trustee and include supporting documentation. File a complaint with the U.S. Attorney and/or the FBI. | U.S trustee in the region where the bankruptcy, U.S. Attorney, FBI in the city the bankruptcy was filed, and you may want to contact the Public Defenders' Office or the State Bar Association in order to find an attorney to help you. |








## 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 also want to get a lawyer to help you.

### STEP 5: 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* 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*.

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


# 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

*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 learning 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.*

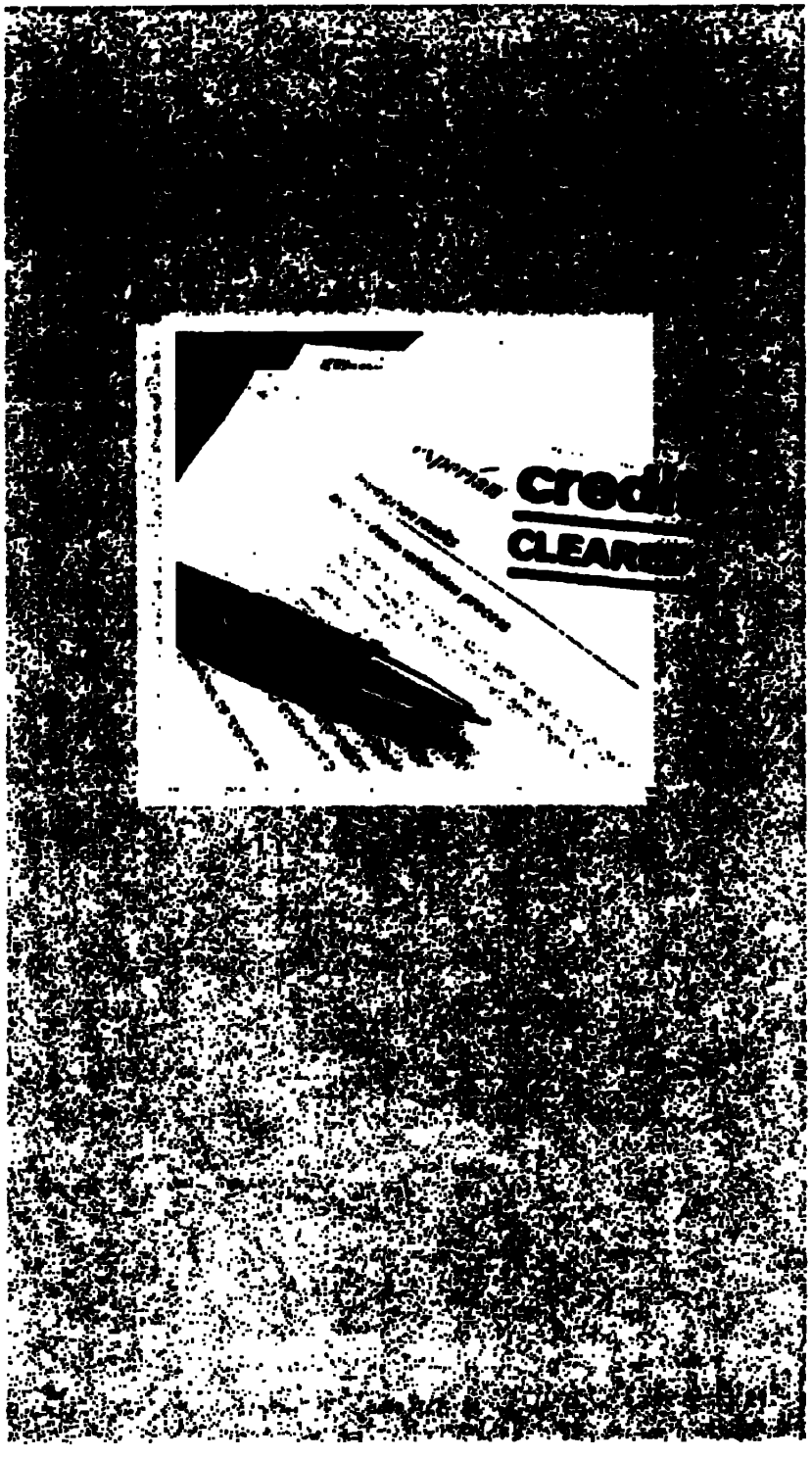
1. Filed a police report.
2. Obtained a copy of your credit report.
3. Identified errors, inquiries you did not know about, accounts you did not open, debts you did not know about, or anything else that seems wrong or out of place on your credit report.
4. Placed a fraud alert on your credit report.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

*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 Number 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.

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

**New Mexico Attorney General's Office**

www.ago.state.nm.us

111 Lomas NW Ste 300
Albuquerque, NM 87102

408 Galisteo Street
Villagra Building
Santa Fe, NM 87501

**For complaints call:**
(505) 222-9000 (Albuquerque)
(800) 678-1508 (In-State Toll Free)
(505) 827-6060 (Santa Fe)
Fax: (505) 827-6685

**For general information call:**
(505) 222-9000 (Albuquerque)
(505) 827-6000 (Santa Fe)

**Federal Trade Commission (FTC)**

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

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

TRANSUNION: 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

**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: Chex Systems, Inc. at 1-800-428-9623 or 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

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/depart/inspect

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

**New Mexico Motor Vehicle Division**

Visit this website to find the MVD service center closest to you: www.state.nm.us/tax/mvd/mvd_home.htm

# ATTACHMENT F

# VETERANS ALERT

The Washington Post

MAY 23, 2006

**"Personal Data on Veterans is Stolen. Burglary Leaves Millions at Risk of Identity Theft."**

New Mexico Attorney General's Office
111 Lomas Blvd., NW, Suite 300
Albuquerque, NM 87102

# Attorney General Patricia Madrid Has Taken Action to Protect Veterans

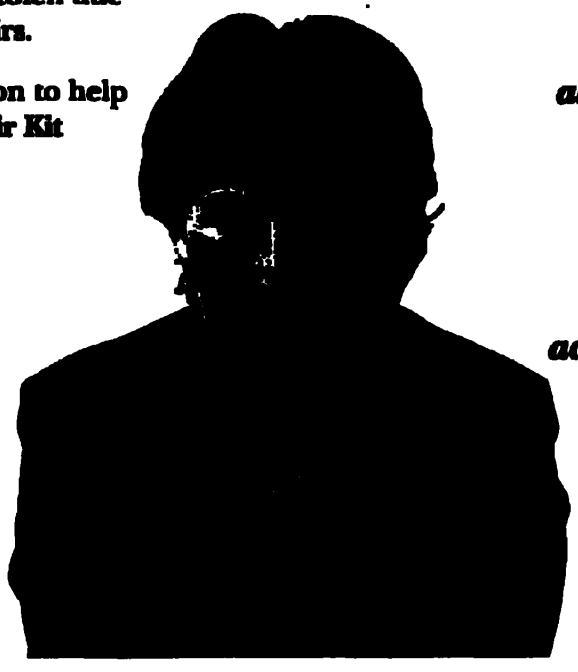
The personal information of 26.5 million veterans has been stolen due to the negligence of the federal Department of Veterans Affairs.

New Mexico Attorney General Patricia Madrid has taken action to help you deal with this crisis by developing an **Identity Theft Repair Kit** that can help you take back your identity.

Right now you should:

- Place a fraud alert on your credit report
- Order a copy of your credit report and check it for anything out of place, such as an account you did not open
- Check recent billing statements and bank accounts for any fraudulent charges or withdrawals
- Regularly monitor your credit report and financial accounts for irregularities.

***Act today to protect yourself from identity theft!***



***"The Department of Veterans Affairs in Washington has allowed the personal information of millions of veterans to be stolen.***

***Here in New Mexico I've taken action to give you the tools to take back your identity and prevent identity theft from happening to you in the future."***

***Patricia Madrid***

## Get your free copy of New Mexico Attorney General Patricia Madrid's Identity Theft Repair Kit

***by calling 505-222-9000 or by downloading the booklet at www.ago.state.nm.us or contact New Mexico Veterans Services at 505-827-6300 (VETS) or www.state.nm.us/veterans***

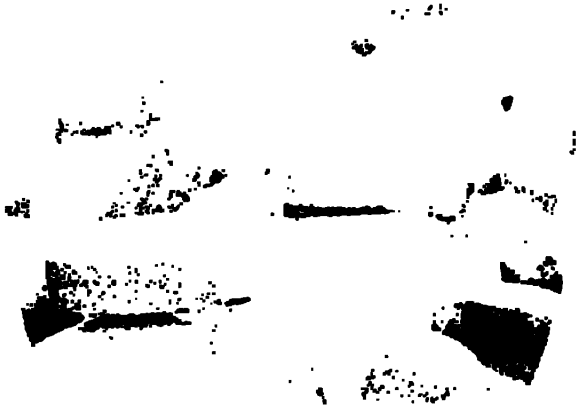
# ATTACHMENT G

# RTION DI
# ING GUIDE

*published by*
**THE STATE OF NEW MEXICO**
**Office of the Attorney General**
**Patricia Madrid**

**www.ago.state.nm.us**
**505-222-9000**

# RTION
# ING GUID



information you can use

*published by*
**THE STATE OF NEW MEXICO**
**Office of the Attorney General**
**Patricia Madrid**

Your medicines have changed.

They are more powerful and more effective.

They are also more expensive.

This booklet can help you save money.

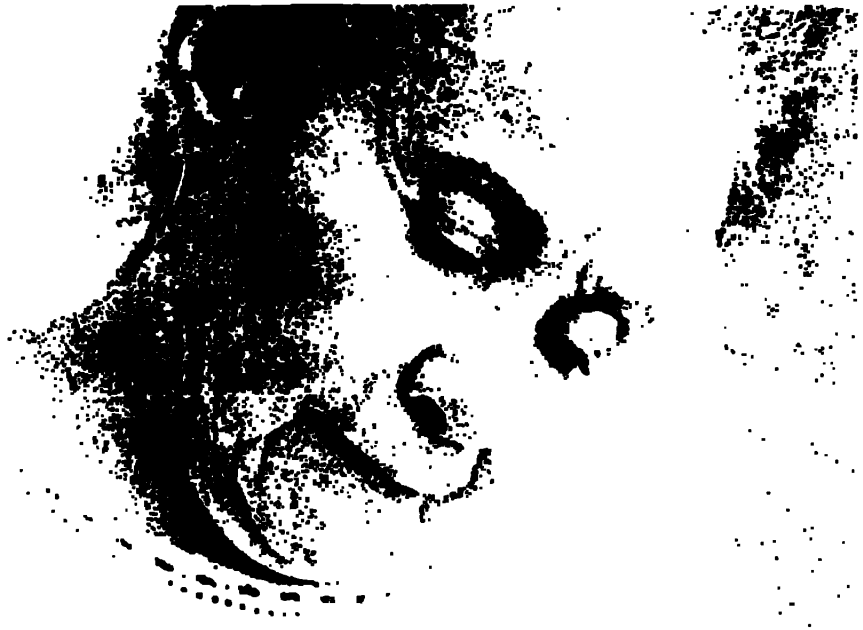
**Message from Patricia Madrid**

Health care advances allow many New Mexicans to maintain a good quality of life in spite of a variety of diseases. But these advances come at a price. For some, the ability to pay for needed prescription drugs is a monthly ordeal.

The prices of prescriptions can vary greatly from one pharmacy to another. If you need to lower the price you pay for prescription drugs, shop around and compare prices and services. Ask if your pharmacy offers any special discounts. Also, you can ask your pharmacy if they will match the lowest price quoted in this booklet or on my website (www.ago.state.nm.us) where even more prescriptions and dosages are priced.

Be sure if you obtain prescriptions from more than one pharmacy that you tell each pharmacy about all the prescriptions you are taking because interactions can be dangerous.

Patricia A. Madrid



## Tips for Helping Your Medication Keep You Healthy

**Don't take old medication. If a prescription is expired, throw it away.**

**Research supplements before deciding to take one. Especially look into supplements or alternative medications advertised as miracle cures, secret formulas, breakthroughs, or a cure to many ailments because they could be bogus.**

**Talk to your doctor and pharmacist before deciding to take any supplements or alternative medicine. Supplements can act in the same ways as drugs, which means they can have dangerous effects if not taken properly. Even vitamins and herbal supplements can have dangerous interactions with your medication.**

**Make sure your doctor and pharmacist know all of the medications you are taking, including prescriptions, herbal or dietary supplements, vitamins, and over-the-counter medications.**

**Did You Know?** You can save money even if you have a prescription drug plan. If you shop around and compare prices, you might find the generic of your prescription for less than your co-pay.

## Treatment for Acid Reflux

Gastroesophageal reflux disease (GERD) or acid reflux disease is a widespread chronic disease. There are many different ways to treat the symptoms of acid reflux. You can treat it with lifestyle modifications, drugs, and/or surgery, if it becomes necessary. There are even different types of drugs for treating acid reflux, such as antacids, histamine receptor antagonists (H2 antagonists), and proton pump inhibitors (PPIs).

Some doctors recommend step therapy for the treatment of acid reflux. A step therapy program can reduce your expenses substantially by starting with lower doses or drugs that are less expensive. Before trying a step therapy approach, remember to talk to your doctor about whether or not it is best for you.

Step-up therapies can involve changing from a lower dose to a stronger dose or from one drug to a stronger drug when symptoms persist. With acid reflux, a step-up approach might be starting with an H2 antagonist and then going to a PPI if the H2 antagonist does not adequately relieve your symptoms. H2 antagonists work by blocking histamine receptors and thus preventing histamine from stimulating acid-producing cells.

Some H2 antagonists are Tagamet (generic: cimetidine), Zantac (generic: ranitidine), Axid (generic: nizatidine), and Pepcid (generic: famotidine). All of these are available over-the-counter or in generic prescriptions, both of which are much less expensive than a brand name prescription.

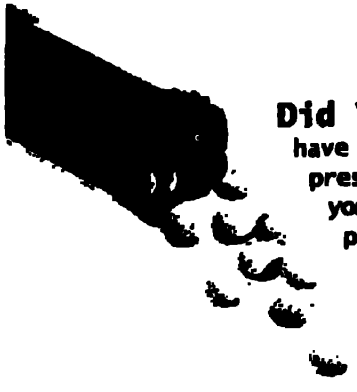
A PPI works by blocking the secretion of acid into the stomach by the acid-secreting cells. Some PPIs are Nexium, Prilosec, Prevacid, Aciphex, and Protonix.

# ACID REFLUX

Brand Names Are In Blue
Generics Are In Red

| Name | Dosages* | Price Range |
|---|---|---|
| Nexium | 20mgCap | $131 to $151 |
| Prevacid | 30mgCap | $128 to $146 |
| Prilosec | 20mgTab | $121 to $137 |
| GENERIC EQUIVALENT | | |
| Omeprazole | 20mgTab | $ 24 to $ 90 |
| Prilosec OTC | 20mgTab | $ 19 to $ 24 |
| Protonix | 40mgTab | $103 to $115 |
| Zantac Tablet(GLX) | 300mgTab | $137 to $153 |
| GENERIC EQUIVALENT | | |
| Ranitidine (PAR) | 300mgTab | $ 9 to $ 37 |

*dosages are priced for 30 units (tablets, capsules) unless otherwise noted



**Did You Know?** Different pharmacies have different prices on the same prescription. You can save money on your prescription drugs by finding a pharmacy with the lowest price or a pharmacy that price matches.

Studies have shown that there are no significant differences in results between most PPIs. Most H2 antagonists will also achieve similar or equal results.

The most popular PPI on the market today is Nexium, also known as the "Purple Pill." Nexium took over the prescription drug market as soon as Prilosec's patent ran out and the generic became available. Nexium was marketed as a much better drug for managing acid reflux than Prilosec. However, studies have shown differently. A study done by the Consumer's Union "indicates that nonprescription Prilosec OTC (omeprazole) is just as likely as prescription PPIs to relieve heartburn and ulcers, and promote healing for most people with gastroesophageal reflux disease." Another study comparing methods of managing GERD done by the Agency for Healthcare Research and Quality found that "PPIs appear to have similar clinical effectiveness when compared to one another for treating GERD." According to these studies, the difference between Nexium and Prilosec OTC is not effectiveness—it's price.

Talk to your doctor about which medication is right for you. Prilosec may treat you as well as Nexium. An H2 antagonist may work as well as a PPI. If the choice is between cutting your costs and the drug most advertised on television, then make sure you are making the right choice. Consult your doctor about brand name and generic drugs. Ask about the differences between H2 antagonists and proton pump inhibitors. Make the smart choice. You do have options.

# ANTIBIOTICS

**Brand Names Are In Blue**
**Generics Are In Red**

| Name | Dosages* | Price Range |
|---|---|---|
| Tetracycline | 250mgCap | $ 4 to $ 6 |
| Augmentin | 500/125mgTab | $149 to $198 |
| GENERIC EQUIVALENT Amoxicillin-Clavulanic acid | 500/125mgTab | $ 49 to $ 99 |
| Biaxin | 500mgTab | $140 to $171 |
| GENERIC EQUIVALENT Clarithromycin | 500mgTab | $ 80 to $143 |
| Cipro | 500mgTab | $166 to $189 |
| GENERIC EQUIVALENT Ciprofloxacin | 500mgTab | $ 29 to $ 83 |
| Flagyl | 500mgTab | $142 to $189 |
| GENERIC EQUIVALENT Metronidazole | 500mgTab | $ 15 to $ 23 |
| Flagyl Er | 750mgTab | $142 to $189 |
| GENERIC EQUIVALENT Metronidazole | 750mgTab | $ 15 to $ 23 |
| Floxin | 400mgTab | $190 to $225 |
| GENERIC EQUIVALENT Ofloxacin | 400mgTab | $122 to $176 |

*dosages are priced for 30 units (tablets, capsules) unless otherwise noted

# ARTHRITIS

**Brand Names Are In Blue**
**Generics Are In Red**

| Name | Dosages* | Price Range |
|---|---|---|
| **RHEUMATOID** | | |
| Arava | 20mgTab | $479 to $514 |
| GENERIC EQUIVALENT | | |
| Leflunomide | 20mgTab | $106 to $250 |
| **RHEUMATOID AND OSTEOARTHRITIS** | | |
| Ansaid | 100mgTab | $ 80 to $ 82 |
| GENERIC EQUIVALENT | | |
| Flurbiprofen | 100mgTab | $ 11 to $ 19 |
| Celebrex | 200mgCap | $ 90 to $ 95 |
| Voltaren | 75mgTab | $ 72 to $ 83 |
| GENERIC EQUIVALENT | | |
| Diclofenac Sodium | 75mgTab | $ 10 to $ 25 |
| Voltaren XR | 100mgTab | $150 to $166 |
| GENERIC EQUIVALENT | | |
| Diclofenac Sodium ER | 100mgTab | $ 35 to $ 80 |

*dosages are priced for 30 units (tablets, capsules) unless otherwise noted

## Tips for Avoiding Health Scams

**Beware of anyone telling you that you have to act immediately. Telemarketers and scam artists may try to tell you that you will lose out on important deals or lose your chance to sign up for insurance or Medicare benefits. Enrollment for Medicare Prescription Drug benefits is strictly voluntary. Do not let a caller convince you that you will lose Medicare benefits if you do not sign up for drug coverage. If you have to sign up immediately, you probably shouldn't sign up at all.**

**Beware of bogus medical, supplemental, or herbal products. Scam artists are continually trying to pass off products as miracle "anti-aging" products or "secret formulas" to curing or preventing Alzheimer's and other diseases or for losing weight. Look for advertising proclaiming "secret formulas", "breakthroughs", or a "cure" for many sicknesses. Just because a product is advertised as safe, natural, and doctor-approved, that doesn't mean it really is. Research any supplement or drug you are thinking of buying and talk to your doctor or pharmacist about it.**

**Did You Know?** Many pharmacies are willing to price match your prescription. Ask your pharmacy if they will match the lowest price in this book or at www.ago.state.nm.us.

# HIGH BLOOD PRESSURE / CONGESTIVE HEART FAILURE

**Brand Names Are In Blue**
**Generics Are In Red**

| Name | Dosages* | Price Range |
|---|---|---|
| **ACE INHIBITOR** | | |
| Accupril | 20mgTab | $ 42 to $ 47 |
| GENERIC EQUIVALENT | | |
| Quinapril | 20mgTab | $ 29 to $ 32 |
| **Altace | 5mgCap | $ 47 to $ 53 |
| **Altace | 10mgCap | $ 56 to $ 61 |
| Prinivil | 20mgTab | $ 32 to $ 43 |
| GENERIC EQUIVALENT | | |
| Lisinopril | 20mgTab | $ 6 to $ 19 |
| Zestril | 40mgTab | $ 54 to $ 61 |
| GENERIC EQUIVALENT | | |
| Lisinopril | 40mgTab | $ 11 to $ 24 |
| Vasotec | 10mgTab | $ 33 to $ 35 |
| GENERIC EQUIVALENT | | |
| Enalapril | 10mgTab | $ 7 to $ 19 |
| **ALPHA-ADRENERGIC BLOCKER** | | |
| Cardura | 4mgTab | $ 41 to $ 44 |
| GENERIC EQUIVALENT | | |
| Doxazosin | 4mgTab | $ 11 to $ 23 |
| Hytrin | 10mgCap | $ 64 to $ 70 |
| GENERIC EQUIVALENT | | |
| Terazosin | 10mgCap | $ 7 to $ 26 |

*dosages are priced for 30 units (tablets, capsules) unless otherwise noted

| | | |
|---|---|---|
| **ANGIOTENSIN II RECEPTOR ANTAGONISTS** | | |
| Cozaar | 50mgTab | $ 50 to $ 59 |
| Diovan | 160mgTab | $ 56 to $ 67 |
| Diovan HCT | 160/12.5mgTab | $ 63 to $ 71 |
| **ANTIPLATELET AGENT** | | |
| Plavix | 75mgTab | $124 to $133 |
| **BETA-BLOCKER** | | |
| Tenormin | 100mgTab | $ 66 to $ 67 |
| GENERIC EQUIVALENT | | |
| Atenolol | 100mgTab | $ 6 to $ 8 |
| Lopressor | 100mgTab | $ 52 to $ 53 |
| GENERIC EQUIVALENT | | |
| Metoprolol | 100mgTab | $ 8 to $ 8 |
| Toprol XL | 50mgTab | $ 26 to $ 32 |
| **CALCIUM CHANNEL BLOCKER** | | |
| Cardizem CD | 180mgTab&Cap | $ 48 to $ 62 |
| GENERIC EQUIVALENT | | |
| Cartia XT | 180mgTab&Cap | $ 31 to $ 37 |
| **CALCIUM CHANNEL BLOCKER AND ACE INHIBITOR** | | |
| Lotrel | 5/10mgCap | $ 70 to $ 82 |
| **CALCIUM CHANNEL BLOCKER** | | |
| Verapamil SR | 120mgTab | $ 6 to $ 22 |
| **Norvasc | 10mgTab | $ 62 to $ 71 |
| Procardia XL | 60mgTab | $ 80 to $ 99 |
| GENERIC EQUIVALENT | | |
| Nifedipine | 60mgTab | $ 19 to $ 60 |

**will go generic within 2 years

**HIGH BLOOD PRESSURE / CONGESTIVE HEART FAILURE (cont.)**

| Name | Dosages* | Price Range |
|---|---|---|
| **CARDIAC GLYCOSIDE** | | |
| Lanoxin | 250mcgTab | $ 7 to $ 9 |
| GENERIC EQUIVALENT | | |
| Digitek | 250mcgTab | $ 4 to $ 5 |
| **DIURETIC** | | |
| Dyazide | 37.5/25Cap | $ 23 to $ 26 |
| GENERIC EQUIVALENT | | |
| Triamterene/HCTZ | 37.5/25Cap | $ 5 to $ 10 |
| Hyzaar | 50-12.5Tab | $ 48 to $ 61 |
| GENERIC EQUIVALENT | | |
| Hydrochlorothiazide | 50mgTab | $ 5 to $ 5 |
| **DIURETIC AND ACE INHIBITOR** | | |
| Prinzide | 20/12.5Tab | $ 37 to $ 47 |
| Zestoretic | 20/12.5Tab | $ 44 to $ 47 |
| GENERIC EQUIVALENT | | |
| Lisinopril-HCTZ | 20/12.5Tab | $ 9 to $ 22 |
| **NITRATE** | | |
| Imdur | 120mgTab | $ 86 to $103 |
| GENERIC EQUIVALENT | | |
| Isosorbide MN | 120mgTab | $ 29 to $ 79 |
| Ismo | 20mgTab | $ 47 to $ 53 |
| Isordil | 30mgTab | $ 22 to $ 22 |
| GENERIC EQUIVALENT | | |
| Isosorbide DN | 30mgTab | $ 9 to $ 10 |
| Monoket | 20mgTab | $ 44 to $ 50 |
| **HMG-COA REDUCTASE INHIBITOR** | | |
| Pravachol | 80mgTab | $138 to $151 |

*Dosages are priced for 30 units (tablets, capsules) unless otherwise noted

## Tips for Avoiding Health Scams

- **Beware of anyone offering free products, such as dietary supplements, in exchange for just a low shipping cost. It could be a scam altogether, the product could be of poor quality or not work at all, or the company could enroll you in a program that ships you more products and then bills you for them.**

- **Research everything solicited to you through telemarketing, emails, and door-to-door sales. Ask for written materials. Do your own research by searching the Internet or checking on a company with the Better Business Bureau.**

- **Never confirm or verify personal information for a person calling or emailing you. A pharmacy or any other legitimate company will not call or email you to confirm your prescription information, credit card number, or social security number. Only provide personal information when you have initiated the contact.**

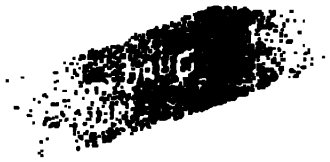
**Did You Know?** A drug in another country might have the same or a similar name of a drug in the U.S., but its active ingredients could be different.

## Tips for Avoiding Health Scams

**Beware of companies offering to help you get medications for free in exchange for a fee. They may claim to be working with pharmaceutical companies to lower the cost of your prescriptions. You could end up paying them fees larger than the cost of your prescriptions and getting nothing in return. Legitimate prescription-assistance programs are free or only require a small processing fee.**

REMEMBER:
You can hang up the phone if you feel threatened, harassed or pressured.

**Did You Know?** You can save money by buying the generic of your brand name prescription. Generics have the same active ingredients as brand name prescriptions, but are typically much cheaper. Like brand name drugs, there may be substantial differences in prices of generics from pharmacy to pharmacy. New generics are introduced frequently, so ask your doctor or pharmacist about their availability often.



# CHOLESTEROL

**Brand Names Are In Blue**
**Generics Are In Red**

| Name | Dosages* | Price Range |
|---|---|---|
| Lescol | 40mgCap | $ 63 to $ 75 |
| Lescol XL | 80mgTab | $ 79 to $ 92 |
| Lopid | 600mgTab | $ 55 to $ 58 |
| GENERIC EQUIVALENT Gemfibrozil | 600mgTab | $ 10 to $ 13 |
| Lipitor | 20mgTab | $103 to $116 |
| Mevacor | 20mgTab | $ 68 to $ 73 |
| GENERIC EQUIVALENT Lovastatin | 20mgTab | $ 14 to $ 32 |
| **Pravachol | 80mgTab | $138 to $151 |
| Questran | 378GMPowder | $ 77 to $ 91 |
| GENERIC EQUIVALENT Cholestyramine | 378GMPowder | $ 38 to $ 40 |
| Vytorin | 10/20mgTab | $ 82 to $ 86 |
| Zetia | 10mgTab | $ 76 to $ 89 |
| **Zocor | 20mgTab | $139 to $148 |

*dosages are priced for 30 units (tablets, capsules) unless otherwise noted

**will go generic within 2 years

# Watch Out For:

"We just need to confirm your personal information."

"You are first required to pay signup fees over the phone (or a website) before we can enroll you."

"This isn't a scam."

"This is a no-risk offer, so there's no need to worry."

"If you don't act now, your Medicare benefits (or other prescription drug benefits) will be cancelled."

"All I need from you is your bank account number (and/or Social Security number, credit card number, ATM PIN number, Medicare card number, health insurance number, etc.)."

"We are an official Medicare representative and we would like to offer you..."

These

## Drug Purchasing Tips

### Questions to Ask Your Doctor:

1. Is this prescription available in a generic form?
2. Is there another option, such as pill splitting or a similar drug, available for this prescription?
3. Is it cheaper and possible for me to buy three-to-six months worth of this prescription at a time?
4. Ask your doctor (or your insurance company) if it is possible to get your prescription by mail.

### Questions to Ask Your Pharmacist:

1. Is there a generic available for this prescription?
2. Is it cheaper for me to buy three-to-six months worth of this prescription at a time?
3. Will you price match or mail prescriptions?

### Tips for Purchasing Prescriptions Online

http://www.ago.state.nm.us/protectcons/prescripdrugs/protectcons_drugs.htm

**Did You Know?** You could save money by pill splitting. Pill splitting is purchasing pills at twice the normal dosage to split in half. If you are considering pill splitting, consult your physician to make sure it is a safe option.

# DEPRESSION

**Brand Names Are In Blue**
**Generics Are In Red**

| Name | Dosages* | Price Range | | |
|---|---|---|---|---|
| Celexa | 40mgTab | $ 83 | to | $ 93 |
| GENERIC EQUIVALENT | | | | |
| Citalopram | 40mgTab | $ 19 | to | $ 42 |
| Effexor | 75mgTab | $ 63 | to | $ 71 |
| Effexor XR | 75mgCap | $ 93 | to | $105 |
| Lexapro | 20mgTab | $ 75 | to | $ 77 |
| Paxil | 30mgTab | $ 91 | to | $103 |
| GENERIC EQUIVALENT | | | | |
| Paroxetine | 30mgTab | $ 26 | to | $ 77 |
| Paxil CR | 25mgTab | $ 86 | to | $ 99 |
| Prozac | 20mgCap | $125 | to | $140 |
| GENERIC EQUIVALENT | | | | |
| Fluoxetine | 20mgTab | $ 7 | to | $ 25 |
| Wellbutrin | 100mgTab | $ 57 | to | $ 70 |
| GENERIC EQUIVALENT | | | | |
| Bupropion | 100mgTab | $ 13 | to | $ 24 |
| Wellbutrin SR | 100mgTab | $ 68 | to | $ 76 |
| GENERIC EQUIVALENT | | | | |
| Bupropion SR | 100mgTab | $ 44 | to | $ 50 |
| Wellbutrin XL | 300mgTab | $124 | to | $149 |
| **Zoloft | 100mgTab | $ 80 | to | $ 89 |

*dosages are priced for 30 units (tablets, capsules) unless otherwise noted

**will go generic within 2 years

# DIABETES

**Brand Names Are In Blue**
**Generics Are In Red**

| Name | Dosages* | Price Range |
|---|---|---|
| **ORAL MEDICATIONS** | | |
| Amaryl | 4mgTab | $ 38 to $ 43 |
| GENERIC EQUIVALENT | | |
| Glimepiride | 4mgTab | $ 10 to $ 36 |
| Avandia | 8mgTab | $164 to $185 |
| Avapro | 300mgTab | $ 60 to $ 73 |
| Diabeta | 5mgTab | $ 26 to $ 27 |
| GENERIC EQUIVALENT | | |
| Glyburide | 5mgTab | $ 9 to $ 11 |
| Glucotrol | 10mgTab | $ 7 to $ 29 |
| GENERIC EQUIVALENT | | |
| Glipizide | 10mgTab | $ 7 to $ 10 |
| Glucotrol XL | 10mgTab | $ 30 to $ 39 |
| GENERIC EQUIVALENT | | |
| Glipizide ER | 10mgTab | $ 15 to $ 39 |
| Glucophage | 500mgTab | $ 25 to $ 26 |
| GENERIC EQUIVALENT | | |
| Metformin | 500mgTab | $ 7 to $ 9 |
| Glucophage XR | 500mgTab | $ 27 to $ 29 |
| GENERIC EQUIVALENT | | |
| Metformin ER | 500mgTab | $ 13 to $ 20 |

| Name | Dosages* | Price Range |
|---|---|---|
| Glynase | 6mgTab | $ 50 to $ 56 |
| GENERIC EQUIVALENT | | |
| Glyburide Micro | 6mgTab | $ 6 to $ 22 |
| **INSULINS** | | |
| Humulin | 70/30 (HI-710)/10ml vial | $ 32 to $ 34 |
| Humulin R | (HI-210) 10ml vial | $ 32 to $ 34 |
| Humulin N | (HI-310) 10ml vial | $ 30 to $ 32 |
| Novolin R | 15 ml vial | $ 20 to $90 |
| Novolin N | 15 ml vial | $ 20 to $ 90 |
| Lantus | 10ml vial | $ 66 to $78 |

*dosages are priced for 30 units (tablets, capsules) unless otherwise noted

**Did You Know?** At warehouse stores, such as Costco and Sam's Club, you do not have to be a member to get your prescription filled at the pharmacy.

## OSTEOPOROSIS

**Brand Names Are In Blue**
**Generics Are In Red**

| Name | Dosages* | Price Range |
|---|---|---|
| Actonel | 35mg (4 pack)Tab | $ 70 to $ 87 |
| Evista | 60mgTab | $ 87 to $ 93 |
| **Fosamax | 70mg (4 pack)Tab | $ 71 to $ 80 |
| Miacalcin Nasal Spray | 200IU (4 pack)Tab | $ 54 to $ 96 |

*dosages are priced for 30 units (tablets, capsules) unless otherwise noted

**will go generic within 2 years

**Did You Know?** At any pharmacy, you could be at risk for short-filling, the practice of billing consumers, Medicaid, or other third party payers for the cost of an entire prescription but only partially filling it, and then asking the consumer to return at a later date to pick up the remainder of the prescription. Sometimes they will not tell you that you have been shorted, so count your pills. Do not pay twice if you have been shorted.

# my prescriptions

**Use this page to keep track of all your prescriptions. Make sure both your physician and pharmacist know all the prescriptions you are taking, even herbal supplements. This is especially important if you get your prescriptions from more than one pharmacy.**

**What I am taking now:** _____ **Date:** _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

# my prescriptions

**Use this page to keep track of all your prescriptions. Make sure both your physician and pharmacist know all the prescriptions you are taking, even herbal supplements. This is especially important if you get your prescriptions from more than one pharmacy.**

**What I am taking now:** _____ **Date:** _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

# ATTACHMENT H

# Spending too much on your prescription drugs?

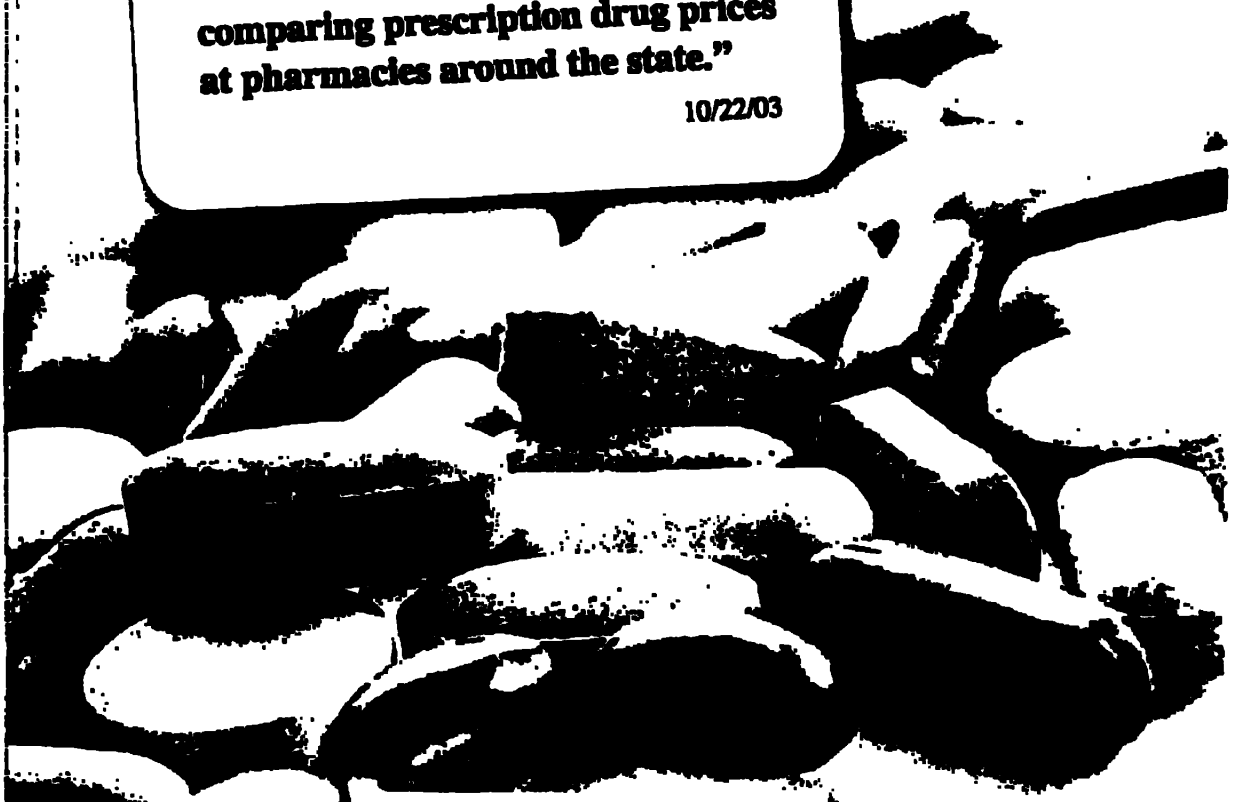
# Attorney Gener

## Fighting to Keep Your

GOOD MORNING AMERICA

"Madrid is attacking drug costs by comparing prescription drug prices at pharmacies around the state."

10/22/03



THE ALBUQUERQUE TRIBUNE

"New Mexico Attorney General Patricia Madrid has created a plan to help people buy drugs at the best prices."

6/19/03

28044222381

# al Patricia Madrid
## Prescription Costs Down

Even as the costs of prescription medications continue to skyrocket, drug companies have resisted efforts to lower their prices. In 2003, Attorney General Madrid took action to help New Mexicans by developing a regularly updated prescription drug pricing initiative that has served as a model for other states. Now the latest drug price comparisons are available to you in book form.

The Attorney General has taken a sampling of drug prices within the state and learned ways to save hundreds or even thousands of dollars. She found savings of up to:

- $3,168 a year by purchasing the generic drug Leflunomide instead of the name brand arthritis medication Arava and an additional $1,728 a year when prices are compared between pharmacies
- $564 a year by purchasing the generic drug Omeprazole instead of the name brand acid reflux medication Prilosec and an additional $792 a year when prices are compared between pharmacies.

***Using generics when available and shopping around to compare prices can save you money!***

**Attorney General Madrid wants to help you learn how to save money on your prescriptions.**

**Send the attached postage-free card today to get your free copy of the Prescription Drug Pricing Guide.**

**Send the attached card today**

***to receive your free copy of Attorney General Madrid's Prescription Drug Pricing Guide***

Dear Attorney General Madrid:

I want to learn how I can save money on my prescriptions.
Please send me a free copy of the *Prescription Drug Pricing Guide*.

Name _____

Address _____

City, State _____ Zip _____

28044222382

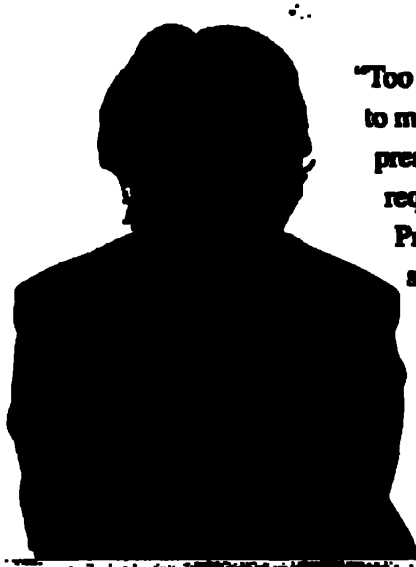
New Mexico Attorney General's Office
111 Lomas Blvd., NW, Suite 300
Albuquerque, NM 87102

U.S. Postage
PAID
Albuquerque, NM
Permit No. 42

**Send the attached card today to receive your free copy of Attorney General Madrid's Prescription Drug Pricing Guide**

BUSINESS REPLY MAIL

ATTORNEY GENERAL PATRICIA MADRID

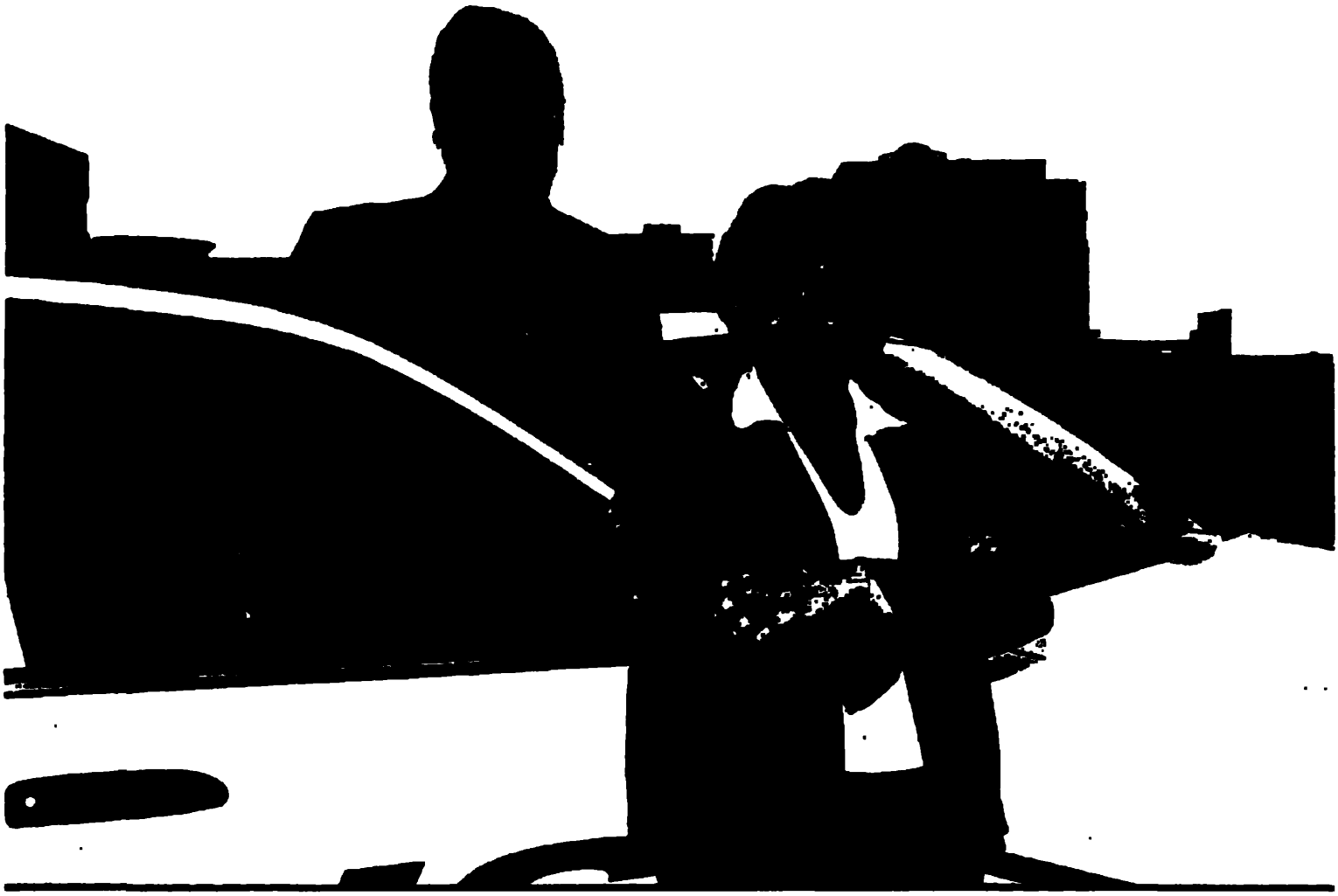


"Too many New Mexicans have to make sacrifices to pay for prescription drugs. Please request your free copy of my Prescription Drug Pricing Guide so I can show you how you can save. You might be able to save money by following a few simple tips."

**Patricia Madrid**

**Learn to save money on your prescriptions by sending the attached postage-free card today or call 505-222-9000 or visit www.ago.state.nm.us to get your free copy of New Mexico Attorney General Patricia Madrid's *Prescription Drug Pricing Guide*.**

# ATTACHMENT I



# Message From

**DANNY ESCOBEDO**
*President, New Mexico Sheriffs' and Police Association*

**PATRICIA MADRID**
*New Mexico Attorney General*

METHAMPHETAMINE isn't just an illegal drug, it's also a toxic danger that affects even those who don't use it. Since the ingredients needed are common and the process to make meth is simple, a meth lab can be set up anywhere, putting you and your neighbors at risk. The chemicals used in meth production can cause fires or explosions and the leftover waste from a lab is toxic. Living near a meth lab is dangerous. We've joined together to inform you how to spot and report meth labs in your area. If you suspect a meth lab, report it immediately using the contact information in this guide.

# Warning Signs

This is an actual photo of the waste a meth lab produces.

## Hazards of a Meth Lab

**Fires** **Explosion** **Health Risks** **Contamination** **Toxic Waste**

- There are a variety of health risks due to exposure to toxic chemicals. You can be exposed to the chemicals from methamphetamine production through skin contact, inhalation, or ingestion, usually from contaminated food or beverages.

- Chemicals used to produce meth contaminate and stay on everything. A house used for a meth lab is still hazardous until trained personnel have cleaned it up.

- Each pound of meth produced creates five to six pounds of toxic waste that meth cooks do not dispose of properly. The toxic waste can find its way onto your street, into your plumbing, your yard, and other places you can be exposed to it.

- Meth cooks often pour the chemical waste from leftover chemicals in storm drains, nearby plumbing, or even right into the ground where the hazardous waste can affect anyone living nearby.

# of a Meth Lab:

## Items you might find in a meth lab:

- Over-the-counter cold medications
- Rubber tubing
- Acetone
- Rock salt
- Funnels
- Gas cans
- Coffee filters with red or white tablet residue
- Fuel containers
- Propane tanks
- Glass containers, such as beakers
- Lye
- Red phosphorus
- Muriatic acid

## Look for combinations of the following:

- Unusual strong or chemical odors like ammonia
- Excessive amounts of trash, especially chemical containers, coffee filters stained red, and other items commonly found in meth labs
- Windows blacked-out, covered in aluminum foil, or with the curtains always drawn
- Increased activity especially at night
- Excessive short-term traffic at unusual times
- Vehicles that sit while someone goes inside for 5 to 10 minutes and then leaves
- Dumping of what looks like chemical waste
- Occupants go to extensive lengths to ensure their privacy
- Empty fuel containers
- Payments for rent or bills are in cash
- Damage to property, such as discolored walls

# WARNING:

**IF YOU SUSPECT A METH LAB IN YOUR AREA, DO NOT INVESTIGATE IT — REPORT IT.**

**THE CHEMICALS ARE DANGEROUS!**

**THE PEOPLE ARE DANGEROUS!**

New Mexico Attorney General's Office
111 Lomas Blvd., NW, Suite 300
Albuquerque, NM 87102





# "Report suspected meth labs immediately."

## They pose a danger to you, your family, and anyone else living near the meth lab.

**Patricia Madrid,** *New Mexico Attorney General*

**Danny Escobedo,** *President, New Mexico Sheriffs' and Police Association*

**Report a suspected meth lab by contacting:**

**Drug Enforcement Agency**
North of Truth or Consequences
(505) 346-7419

**Drug Enforcement Agency**
South of Truth or Consequences
(505) 527-6950

**New Mexico State Police**
1-888-442-6677

**HIDTA Narcotics Regional Task Force**
Chaves County: (505) 623-8010
Lea County: (505) 393-2835
Lincoln County: (505) 258-4798
Pecos Valley: (505) 887-5194
Rio Arriba and Santa Fe counties:
(505) 471-1715
San Juan County: (505) 566-2222

**You can also contact your local police.**

---

This message is brought to you by New Mexico Attorney General Patricia Madrid and the New Mexico Sheriffs' and Police Association.