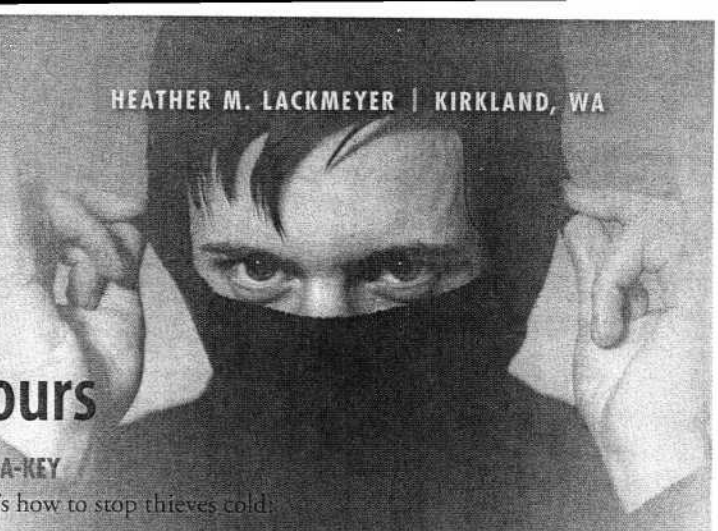
HEATHER M. LACKMEYER | KIRKLAND, WA



# face lift

## keep ID thieves from lifting yours

IMAGINE SOMEONE FALSELY IMPERSONATING YOU – another evil "you" running around, renting an apartment, draining your accounts, even signing up for and maxing out credit cards in your name. This isn't some cheesy sci-fi thriller. This is identity theft, and there are scores of thieves out there who can't wait to live your life to the fullest.

Your identity is your treasure – a handful of key pieces of critical information including your name, Social Security number, address, phone number and your mother's maiden name. Thieves are also after any account numbers or passwords they can use to get access to your money. Here's how to keep your identity safe.

### KEYS TO YOUR CASH

An identity thief can use the information they've collected to:

- Make charges to your credit cards or open new ones
- Counterfeit your checks and clone your ATM/debit cards
- Open accounts or take out loans in your name
- Obtain driver's licenses and receive medical services
- Receive government benefits
- File fraudulent tax returns
- Apply for jobs and rent apartments
- Break the law and blame you

> "YOUR **IDENTITY** IS YOUR **TREASURE.**"

### LOCK IT DOWN

How do thieves get your information? Accessing it electronically is popular, but thieves are not above old-fashioned Dumpster diving. Common methods include:

- Stealing mail or trash and researching public data
- Stealing payment/ID cards or the information on them
- Eavesdropping on public transactions
- Hacking information from corporate databases
- Impersonating an organization or business through email (phishing)
- Viewing information you provide on social networking websites

**HELP!** Identity Theft Resource Center: **idtheftcenter.org**
Privacy Rights Clearinghouse: **privacyrights.org**

### HIDE-A-KEY

Here's how to stop thieves cold:

- Be careful anytime you provide your Social Security number.
- Shred all charge receipts, credit applications, insurance forms, checks, statements, expired credit cards, and credit card offers.
- Choose intricate passwords for your online logins.
- Use a password to protect any sensitive information on your personal computer.
- Implement safety tools such as a firewall or antivirus program on your computer.
- Always verify sources requesting information and only provide what is necessary.
- Be careful about how much personal information you post on social networks like Facebook and MySpace.
- Beware of conducting important business online over free/unprotected wireless networks. Free can mean less security.

**40 HOURS**
THE AVERAGE AMOUNT OF TIME PER VICTIM TO **RESOLVE AN INCIDENCE OF ID THEFT.**
source: privacyrights.org

There are identity protection services such as ID theft insurance that provide coverage based on policy limits. Some only cover certain forms of ID theft, like electronic theft, while others cover lost wages. Visit ftc.gov to learn more.

### CHECKING THE LOCKS

Identity thieves can run up bills you'll often be responsible for, and if you don't discover these charges until they go into delinquency, your credit score could suffer too. Fortunately, in most cases, the largest cost of ID theft is clearing your name. Prevention and detection are key defenses. Always review your account statements for changes or purchases you didn't make. Check your credit report at least once per year (free at annualcreditreport.com) for any suspicious activity.

**get more**
**[AT BRASSMAGAZINE.COM]**
Already been hacked? Check out our **online exclusive** this month for three steps to take if you are a victim of ID theft.

---

BOTTOM LINE: There were 8.4 million victims of identity theft in the U.S. in 2007 and losses hit $49.3 billion. ID theft is real, but the best defense against it is to be careful with your personal information.