

CLIENT TELL

AS THE HOLIDAYS APPROACH, SAFEGUARD YOUR IDENTITY

Each year millions of American consumers fall prey to identity theft. This is particularly true during the winter holidays, when crowds increase and our minds are occupied by gift giving and celebration. But a few simple prevention tactics could save you thousands of dollars, not to mention unnecessary time and aggravation. To safeguard your identity throughout the year:

Protect your Social Security number. Don't carry it in your wallet or write it on a check. If your State or health insurance company uses your Social Security number as your driver's license number or policy number,

ask them to substitute a different number instead. Never give out your Social Security number without first determining who needs it and why. Before providing it, always ask: Why do you need my Social Security number? How will it be used? How will you protect my Social Security number from being stolen? What will happen if I don't give it to you? Remember: The decision to share this information is *yours* and yours alone.

In public, keep your personal information private. Before going shopping, plan ahead: Only carry the personal identification info and credit or debit card

(Continued on Page 3)

Your Social Security number is like a password to your personal information. That's why safeguarding it is crucial. Left unprotected, your computer also serves as a personal data portal. It's important to keep it secure from ID thieves and hackers.

Know the dangers. The Internet makes it easy to access various types of information and infinite services. But it also leaves us vulnerable to increasingly sophisticated scams. To keep current on the risks involved, routinely visit www.OnGuardOnline.gov. This FTC-managed website offers information and practical advice on recent and ongoing scams and security topics.

(Continued on Page 3)

GIFT YOURSELF

Staying on budget and making debt management plan (DMP) payments on schedule can be tough during the holidays. But sticking to these financial priorities will make it easier to greet 2009 with a smile. Whether you pay online, by ACH, or by money order, make your DMP payments on time and in full.

On money orders, please print all info legibly. List *CCCS of MD & DE* in the "Pay to Order Of" blank. List your address and phone number below your signature and your client number in the corner of the money order. Sign the money order and enclose the top portion of your statement. Keep the receipt for future reference. And have a joyful holiday season!

Inside this issue:

Safeguard Your Identity	1
From the President	1
Gift Yourself	1
From the Trenches	2
If You're a Victim of ID Theft	2
Voters Beware	2
Ask a Counselor	4
Parting Thoughts	4

FROM THE TRENCHES

by **Kathy Skidmore-Williams**

It's mid-September as I write this, and my local "big-box" store already has two big aisles devoted to holiday decorations. Not Halloween decorations, not Thanksgiving decorations, but Christmas decorations! At least the piped-in music isn't "Jingle Bells"—yet! I have a feeling with all the dire financial news, merchandisers are getting concerned their holiday sales will be down so they're going overboard early. I know sales will be down from me because I don't have extra cash to spend and I'm determined not to overextend, though the pressure grows to do just that.

It can be hard work bucking the barrage of commercials and peer pressure, but, by being imaginative with our gift giving, we earn two things: we don't go into debt, and we have the chance to give something meaningful and creative to someone we care about. When I worry about what that someone might think of a gift that's inexpensive or homemade, I try to put myself in the place of that someone. How would I feel if I got something like that from a friend? Would I care about him or her any less? Of course not! Chances are, I'd remember that gift all the more for the time and thought that went into it whether it was a tin of cookies or a heartfelt note. A little ingenuity can take you a long—and debt-free—way.

IF You're a Victim of ID Theft

Place a fraud alert on your credit reports. Call the toll-free fraud number at Equifax, Experian, and TransUnion. After you place a fraud alert on your files, you will be entitled to receive free copies of your credit reports. Carefully review each one. Check for inquiries from companies you didn't contact, accounts you didn't open, and debts on accounts you can't explain. Also verify that information like your name or initials, SSN, address, and employers are accurate. If you find inaccurate or false information, ask that it be removed.

Close accounts that were opened fraudulently or tampered with. Call and speak to someone in the security or fraud department of each company and follow up in writing. Include copies of supporting materials, and send these letters by certified mail with return receipt requested. If the ID thief has made charges or debits on your accounts or fraudulently opened new ones, ask the company for forms to dispute these transactions. If you open new accounts, use new Personal Identification Numbers (PINs) and passwords.

File a local police report. Request a copy of the report and retain it for your records. Credit card companies and financial institutions may ask to see it to verify the crime.

File a complaint with the FTC. This will help law enforcement officers combat ID theft across the nation. You can file an online complaint at: www.consumer.gov/idtheft or call the FTC's Identity Theft Hotline, toll-free at: 1-877-ID-THEFT (1-877-4338) / TDD 202-326-2502.

VOTERS BEWARE

With election time just around the corner, scammers are now masquerading as members of your local election board or reputable civic groups.

How it works: You receive an email, a telephone call, or even a visit from a sunny, sincere paid volunteer who offers to help you register to vote. Only one problem — they need personal information to register you as a new voter or verify your current voting eligibility.

The straight scoop: Identity theft is the true objective here. If you provide the scammer with your Social Security number or credit card or bank account numbers, this info will be used fraudulently, and before you know it, your identity and financial well being will be compromised.

What to do instead: Make your voice heard through your vote. If you haven't already registered, promptly fill out a voter's registration form. For information on how to obtain one, check with a local post office or public library near where you live.

SAFEGUARD YOUR IDENTITY

(continued)

you actually need. When standing at a cash register, shield your card or check from other people's view. Throughout the transaction, pay attention to the cashier's actions.

Verify phone and Internet sources. Identity thieves are smart: They may pose as representatives from banks, government agencies, or Internet service providers. Unless you have initiated the contact or know exactly with whom you're dealing, do not reveal information like your Social Security number, mother's maiden name, or account numbers.

Before sharing personal information, confirm that the organization requesting it is legitimate. Ask phone contacts for an address and background details. Then call the Better Business Bureau to verify what you've learned.

Beware of email requests for personal data. Before responding, verify the group's website. Often reputable companies post scam alerts when their name has been used improperly. To check

if an organization's site is legit, type its URL in the address box on your browser. Do not click a link or cut and paste the web address directly from the email you received as this may lead you to a fraudulent site.

Handle your mail and trash with care. These two locations are treasure trove to identity thieves in search of vital information. Promptly remove your mail from your mailbox each day. If you plan to be away for an extended period, contact the U. S. Postal Service at **1-800-275-8777** or online at **www.usps.gov** to request a vacation hold. Don't leave mail that contains personal information for pick up in an unsecured mail box. For increased security, mail it directly from a local post office instead.

Always shred items such as charge receipts, copies of credit applications, credit offers, checks, and bank statements, insurance forms, or physician statements before disposing of them in the garbage.

None of these measures requires immense amounts of time or effort. By getting into the habit, you help insure that your identity will stay your own!

FROM THE PRESIDENT'S DESK (continued)

Choose an intricate password for online accounts. Avoid using information that's easily available, such as your birth date, the last four digits of your Social Security number, your mother's maiden name, a single word that is found in the dictionary, or a series of consecutive numbers. Combinations of numbers, letters, and special characters make the best passwords.

Install reputable anti-virus and anti-spyware software and firewalls. The OnGuardOnline.gov website contains a list of tools from legitimate security vendors. Whenever possible, set your security software to update automatically. That way, it will stay protected even when you're in a time crunch such as at holiday time.

Don't reply to emails, text, or pop-up messages that request personal or financial information. Also avoid clicking on links from these messages or responding if they ask you to call a phone number to update your account or give personal info for a refund. Instead, go directly to a bank or business's website, and type the site address into your browser yourself — or use a telephone directory to locate the phone number. If you need to reach a business or organization with which you already do business, call the number listed on your statement.

Report deceptive spam. Forward any scam emails you receive to **spam@uce.gov**. Include the full header of the email as well as all routing info. The time you take may make someone else's holiday season safer and happier!

Ask a Counselor

Q: When I need help, I often contact CCCS by email. Is it also okay to send you personal information by email?

A: Contacting CCCS by email is great, because it's fast and inexpensive. But it isn't safe to send personal information over the Internet. Never email us full account numbers for your credit or checking accounts — or other pieces of vital personal information. When this type of data is needed, call (1-800-571-2227), fax (410-869-8828) or mail it to us instead.

Parting Thoughts

Make a Positive Difference. Given the state of the economy, lots of us are struggling just to make ends meet — and many have fallen behind. If you know a family member, friend, or co-worker who is in serious debt or facing foreclosure right now, why not share your experience and insight? We also want to help. Please feel free to give them CCCS's phone number (1-800-642-2227) and encourage them to visit our website (www.cccs-inc.org). Together we can provide help in hard times.

Free Annual Credit Reports. One way to avoid identity theft is to regularly review your credit report. You're even entitled to receive a free one each year from each of the three major credit reporting agencies — Transunion, Experian, and Equifax. To request your free, annual credit report from all three, access www.annualcreditreport.com and fill in the simple required form.

Older & Wiser. Seniors are often targeted by scam artists and identity thieves. If you or someone you care about is a member of the "grey generation," you may wish to request a copy of the MD Office of Attorney General's comprehensive "Consumer Guide for Seniors." It includes information on several common consumer, health, and financial scams as well as a host of helpful resources. To get your free copy, simply call 1-888-743-0023 or visit www.oag.state.md.us. Excellent information also is available on the AARP website (www.aarp.org).

A personal finance education advocate since 1966.



757 Frederick Road
Baltimore, Maryland



Non-Profit Org.
U.S. Postage
PAID
Annapolis, MD
Permit No 273