PFPG BRIEF

PORTLAND FINANCIAL PLANNING GROUP, LLC

Identity Theft

511 Congress Street, Suite 804, Portland, ME 04101
Tel: (207) 771-8821

PREVENTION

- **Protect your financial accounts** (brokerage, bank, credit card, and employer benefits) with **strong security codes and passwords** (**https://howsecureismypassword.net/**) that don't reference your personal information. Longer is stronger. If you have difficulty keeping track, use a password manager such as **LastPass** (available in a free version). Change your passwords on a regular basis.
- Set up **two-part authentication** for online accounts wherever possible. Avoid creating security questions for which a thief could find the answers online (e.g. where you were born, high school mascot). Make up false/outlandish answers, but keep track of them!
- To prevent potential creditors from accessing your credit history files and from granting instant credit to thieves, contact the three credit-reporting agencies to place **security freezes** and **fraud alerts**. See: **www.consumer.ftc.gov/articles/0497-credit-freeze-faqs**.
- **Check your credit report** at least once a year. Stagger your requests to the three major credit agencies so you receive a report every four months. If you've been a victim, review it quarterly. Be aware of "imposter" websites that claim to offer free credit reports or other credit report monitoring services. Only one website is authorized to fill orders for the free annual credit report under law – **www.annualcreditreport.com.** The jury is out on credit monitoring services. For now, it is hard to recommend any.
- Pay attention to billing cycles and statements, and **review statements each month**. Contact the creditor if a statement doesn't arrive.
- Update computer virus protection regularly, and use anti-malware software if you suspect an undetected infection. Use a hardware or software firewall which prevents hackers from accessing your computer. (Make sure to enable Windows Firewall on your PC.) Limit banking activities to a hard-wired home connection.
- Do not use links in an e-mail to navigate to a financial institution's Web site. Chances are high that it is a "phishing" e-mail that will lead you to a phony site.
- Store files with personal information in a safe place. Encrypt computer data, including backup files, with a program such as WinZip. Don't keep unsecured financial information on your computer(s). Shred documents containing personal data and preapproved credit card offers before you discard them.
- Carry a minimal amount of personal information with you, and limit the number of credit cards in your wallet. Keep copies (front and back) of all cards carried in your wallet in a safe place in case your wallet is stolen.
- Personalize your bank checks only with your first initial and last name (exclude your mailing address).
- Don't give out any personal information via phone, mail or internet unless you initiated the contact.
- When asked to provide personal data, verify that the information is essential. Ask questions such as: "Why do you need my Social Security number?", "How will it be used?", "How do you protect my Social Security number from being stolen?", or "What will happen if I don't provide my Social Security number?"
- If you are notified by the IRS that a second return has been filed with your Social Security number, file Form 14039 with the IRS immediately and take all suggested steps below. And remember – the IRS will never contact you by phone or e-mail about past due payments, etc., only by mail.
- Opt out from direct mailing lists, sign up with the national Do-Not-Call Registry, and opt out of pre-approved credit card offers (*see Resource Table on the 2nd page*).

IF YOU'VE BEEN VICTIMIZED

- Immediately call your respective financial institutions to cancel your credit and debit cards. Your potential liability may depend on how soon you reported the crime. The Federal Trade Commission's step-by-step guide "Taking Charge: What to Do if Your Identity is Stolen" can be downloaded at **www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf**. A useful checklist and links to other resources are also provided on the **Privacy Rights Clearinghouse website**.
- Our clients should contact us for advice and assistance.
- File a report with local police. If identity theft is not a crime under your state law, ask to file a Miscellaneous Incident Report instead. If the local police won't take a report, contact state police.
- Document all of your communication relative to ID theft: dates, times, institutions and individuals contacted. It is best to contact financial institutions, credit-reporting agencies and other fraud-related companies in writing, so that your requests and claims are on record with the recipients.
- Call the fraud units of the three major credit reporting agencies (*see Resource Table*).

PFPG BRIEF

PORTLAND FINANCIAL PLANNING GROUP, LLC

Identity Theft

511 Congress Street, Suite 804, Portland, ME 04101
Tel: (207) 771-8821

- To make certain that you're not responsible for any debts incurred by identity theft, you must prove to creditors that you didn't accumulate the debt. Fill out the FTC's **Identity Theft Victim's Complaint and Affidavit** which is widely accepted by creditors.

RESOURCE TABLE

Annual Credit Report: Request free annual credit report	To order online, **www.annualcreditreport.com;** for credit report request mail-in form, follow the link: **https://www.annualcreditreport.com/gettingReports.action**
Credit Offers: Opt out from pre-approved credit offers	888-5-OPTOUT (67-8688) or **www.optoutprescreen.com**
Computer Security	See the Federal Trade Commission's website for a comprehensive guide: **www.consumer.ftc.gov/topics/computer-security**
ID Theft: Credit freeze and fraud departments of credit-reporting agencies	**TransUnion:** 800-680-7289; **www.transunion.com** or Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA 19016. For credit freezes: 888-909-8872. **Equifax:** 800-525-6285, **www.equifax.com** or Fraud Division, P.O. Box 740241, Atlanta, GA 30374- 0241. For credit freezes: 800-349-9960. **Experian**: 1-888-EXPERIAN (397-3742); **www.experian.com** or Fraud Division, P.O. Box 2104, Allen, TX 75013. (Write to avoid Experian's marketing pitch for "free" credit management tools.) For credit freezes: 888-397-3742.
File a complaint (affidavit) with the Federal Trade Commission	The FTC's website is **ftc.gov/complaint.** Follow the step-by-step menu for the **FTC Complaint Assistant.**
Resources on ID Theft	**www.privacyrights.org** **www.maine.gov/ag/consumer/identity_theft/identity_theft.shtml** (Maine ID theft laws and resources) **www.ftc.gov** **www.onguardonline.gov**
Social Security Fraud: Report misuse of Social Security number	Contact the Federal Trade Commission in the event that someone uses your Social Security number to obtain credit, loans, phone accounts, or other goods and services.
Direct Mail / E-mail Marketing: Remove name from catalog/magazine offers and other solicitations	Use the Direct Marketing Association's free online mail management service to reduce catalogs, magazine offers, and other forms of direct mail solicitation at **www.dmachoice.org.** The DMA also has an e-mail Preference Service (eMPS) on the same site. By mail only, download the form and write to: DMAChoice, Direct Marketing Association, PO Box 643, Carmel, NY 10512. There is a $1 processing fee for mail-in requests.
Direct Mail: Reduce mail order catalog flow	E-mail your request to **optout@epsilon.com** or write to Epsilon Data Services, P.O. Box 1478, Broomfield, CO 80038. Include full name and current address (and previous address if you have recently moved.)
Phone Marketing: Remove name from telemarketing lists	To be removed from phone solicitation lists, register online at **www.donotcall.gov,** call 1-888-382-1222 from the phone you want to register, or write to Telephone Preference Service, Direct Marketing Association, PO Box 1559, Carmel, NY 10512 (telemarketers have up to 31 days to comply). Companies you do business with will not be removed, however.