

Grab-N-Go return policy.

We will refund the full purchase price, less shipping charges, for Grab-N-Go product returned within 30 days of purchase. The Grab-N-Go product must be a) in unused resalable condition and b) shipped in a protective carton to protect the printed packaging. Prior to any returns, you must call 404-273-8348 for a Returned Merchandise Authorization (RMA) number, which must then be written on the returned product shipping label.

Shipping

Grab-N-Go orders are shipped via UPS Ground and delivery usually takes from 3 to 7 business days.

Grab-N-Go Internet Privacy Statement

Grab-N-Go respects your privacy and is committed to protecting it at all times. This Internet Privacy Statement explains how we collect, use, and safeguard information on this website. Effective Date: 05/1/07

Information We Collect About You Online

We want you to get the most out of your visits to our website. From offering special promotions to new users. To provide our users with these and other online tools, we will, from time to time request that you provide us with your personal information, such as your name, address, email address and telephone number. **Website users:** We will ask you for certain contact information when you register for online services and products.

1. We will ask you for certain personal information if you want to order your products online. In some instances, we will need to supplement the information you provided with certain personal information about you obtained from third parties to process your online transaction, such as a credit card processing when paying for the product on our shopping cart.

We will maintain information about your account, online account activity, online services and products requested and your usage of our website to help us administer your online account needs and to continually improve your online experience by providing you with customized, relevant information and offers.

How We Use The Information We Collect

Whether you are a new website user or a customer, we use personal information collected on our website to handle the transactions you initiate. In some instances, we will share

your contact information with carefully selected service providers to assist us in processing your online transactions or to deliver the services products you request online. For example, in order to mail you the financial guide you request online, we will supply your contact information to a third party vendor who will process and mail the product,

Tracking Activity On Our Website

In order to make your visit to our website as productive as possible, we track activity on our website. However, we want you to know that the tracking technology we use does not identify any personal information about you. They cannot retrieve data from your hard drive, pass on computer viruses, or capture any personal information about you, such as your name, address, phone number, or email address. We only know who you are if you tell us. You may, however, be asked to provide personal information such as name, address, phone number or email address to us when you register for online services or products.

1. **Cookies:** One way we track activity is by using cookies. A "cookie" is an electronic file that holds small strings of text. When you visit our website, we send a cookie to your browser so that we can recognize it when you or another user of your computer return to our website. We want to recognize your browser so we can make the best use of your time when visiting our website. For example, when you visit our website, we present an introductory page to all new users. The fact that you have already visited the introductory page is recorded in a cookie so you won't see the introductory page again. For your security, if you are registered for online services and/or have an account we can not give you access to your account information on our website unless your browser is set to accept cookies from us.
2. **Advertising:** When you visit our website by clicking on certain banner ads or special offers on our partners' website, we track this information to improve navigation and deliver relevant information when you arrive at our website. We also do this because we want to determine if our ads and special offers are appealing to our users.

In the course of serving our ads to you, a unique third-party cookie may be placed or recognized on your browser. In addition, we use web beacons, provided by our third-party ad server, to help manage and optimize our online advertising. These web beacons enable us to learn which ads we place on third-party sites bring users to our website. They do not capture or convey any personal or sensitive information about you.

3. **Browser settings:** You can adjust many browser preferences so that you are alerted when a cookie is placed in your browser, or adjust preferences to decline cookies altogether. Recognize that cookies enable you to visit our website without reviewing introductory information. In addition to allowing us to recognize you, cookies also enable us to securely provide our registered users with account information.

How We Use Your Email Address

We recognize that email can be the preferred mode of communication for some of our website users. If you provide us with your email address when registering for an online service or product or when accessing your account online, we will use it to contact you about online services and products for which you have registered or about your account.

We may use your email address to send you the following types of email messages:

- Service notifications related to your accounts(s)
- Occasional updates about our products and services. Valuable offers from non-affiliated companies that we send you on their behalf

Also, once you have requested information or order from us, we may communicate with you via email regarding your request to provide additional information related to your initial information request.

We do not share your email address with non-affiliated companies for them to market their products or services directly to you. However, we may partner with selected non-affiliated companies to offer certain products or services we believe may be of interest to you.

You may receive email offers from other companies for Grab-n-Go products and services if you registered to receive third-party offers on their website, or if you receive ongoing email newsletters from the other companies that include third-party ads. If you have recently opted out of receiving email offers from Grab-N-Go financial organizer, we will process and honor your request as soon as administratively possible. In certain circumstances, you may receive email offers for Grab-n-Go financial organizer and services from other companies during the time period when we are processing your opt-out request.

To opt-out of receiving offers or email newsletters from other companies, follow the instructions provided by those companies.

Ads That Link To Our Website

Grab-n-Go financial organizer may use third parties to place banner ads on other websites and will perform tracking and reporting activities through use of Ad Servers. We do not provide Ad Servers with your personal information and Ad Servers do not collect your personal information.

Ad Servers are subject to their own privacy policies. If you would like more information about the privacy policies of these Ad Servers, including information on how to opt-out of their tracking methods, please [click here](#) to visit the Network Advertising Initiative website.

Your Opt-Out Choices

We strive to send you email communications that are informative and relevant, but also appreciate that you are in the best position to evaluate the type and frequency of our communications to you.

To opt-out of receiving email offers or newsletters, [click here](#). All email offers and email newsletters sent to you by Grab-n-Go financial organizer provide instructions on how to opt-out of receiving future offers or newsletters. These instructions are located at the bottom of the email message. If you opt-out, we will still send you email with service updates as well as other important information related to the Grab-N-Go products or services for which you have signed up.

How You Can Protect Your Personal Information

Identity Theft 101

Identity theft occurs when someone uses your name or personal information, such as your Social Security number, driver's license number, credit card number, telephone number or other account numbers, without your permission. Identity thieves use this information to open credit accounts, bank accounts, telephone service accounts, and make major purchases — all in your name. Information can be used to take over your existing accounts, or to open new accounts. Identity theft can result in damage to your credit rating and denials of credit and job offers.

EXAMPLE #1 - One evening, you sit down to pay your monthly bills. You write the checks, toss the statements in the trash and put the container out on the curb for the morning's trash pick-up. While you sleep, "dumpster-divers" go through your trash looking for the papers you've thrown away. They discover a gold mine of information that can be used for fraudulent purposes — your name, address, phone number, utility service account numbers, credit card numbers, and your Social Security number.

EXAMPLE #2 - You receive an email message from what appears to be your Internet Service Provider (ISP). The message requests that you update the information they have on file about you — your name, credit card number, bank account number, etc. — by replying to the email or going to a specific website address to provide the information. However, neither the message nor the website address is from your ISP. They belong to someone who wants to get your information to steal your identity.

Preventing Identity Theft

1. **Secure your personal information at home and at work.** Consider keeping your sensitive personal information such as bank, mortgage, and credit card

statements, Social Security cards, and other documents and passwords, in a safe location accessible only to you.

2. **Protect yourself online:** Avoid accessing your accounts online from public computers at libraries, hotel business centers or at airports. These are prime target areas for thieves using keystroke monitoring tools to steal your usernames and passwords. Use firewalls, anti-spyware and anti-virus software to protect your home computer and regularly update these programs.
3. **Shred documents containing your personal information before discarding them.** Identity thieves have been known to “dumpster dive” to obtain discarded documents with personal information.
4. **Obtain your credit report from each of the three major credit bureaus once every six to 12 months.** Review these reports for any inaccurate information, or any transactions that you were not aware of or did not authorize. You may wish to consider occasionally reviewing Credit Bureau Reports on your children. Identity thieves have been known to steal children's Social Security numbers in order to create fraudulent accounts, as their information is not likely to be reviewed regularly.
5. **Avoid giving out personal information over the phone** especially when the telephone call is initiated by another party. Identity thieves may pose as a representative of a legitimate organization with whom you do business and may contact you to "verify" your information.
6. **Before disclosing any personal information,** make sure you know why it is required and how it will be used.
7. **Do not give out your Social Security number** to people or companies that you do not know.
8. **Carry only the information you need.** Only take with you the credit cards you need, and avoid carrying your Social Security card, your birth certificate or passport, except when necessary.
9. **Have the Postal Service hold your mail if you are going to be gone for a few days or more.** Since identity thieves have been known to obtain personal information by collecting an individual's mail, promptly remove your incoming mail from your mailbox and place outgoing mail in post office collection boxes. Have the Postal Service hold your mail at the post office if you are planning on being away for any period of time. Install a locking mailbox if mail theft is a problem in your neighborhood.
10. **Create unique passwords and personal identification numbers (PINs)** and avoid using easily available information such as mother's maiden name, date of birth, or the last four digits of your Social Security number. Use passwords on your banking and brokerage accounts, and update all of your passwords regularly.

If you need further guidance, you may wish to consult the consumer affairs office of the company involved, the U.S. Better Business Bureau, or your local or state consumer protection agency.

Detecting Identify Theft

Fortunately, detecting identity theft can be fairly simple for diligent consumers. Just follow these three steps:

1. **Contact the Credit Bureaus**

First contact each of the three national bureaus and request copies of your credit report.

EQUIFAX

Order Credit Report: (800) 685-1111

www.equifax.com

EXPERIAN

Order Credit Report: (888) 397-3742

www.experian.com

TRANS UNION

Order Credit Report: (800) 888-4213

Fax: (714) 447-6034

www.transunion.com

2. **Review Your Credit Reports**

Review all three of your credit reports carefully and make sure you:

Recognize all accounts listed in your report and confirm that the balances are in line with your records.

- Recognize all persons and entities that have requested or received a copy of your report. (If you do not recognize a person or entity, you may want to inquire further).
- Find no inquiries to your credit report for loans or accounts you did not apply for. (If there are accounts you do not recognize, this may be a sign that an identity thief has fraudulently opened an account in your name).
- Confirm there are no addresses listed for places you have never lived. (If there are addresses you do not recognize, this may be a sign that an identity thief has redirected your mail).
- Check that your Social Security number and employment history are accurate.
- Check that all this information is consistent across all three credit bureaus.

3. **Correct Your Information**

If you find any incorrect or suspicious information, contact the credit bureau(s) immediately. If the incorrect or suspicious information concerns a particular creditor, you will want to contact that creditor as well.

Restoring your good name

These step-by-step guidelines were developed by the FTC, and are provided by Grab-N-Go financial organizer to help you repair the damage caused by identity theft. Here you'll find contact information on the relevant authorities, forms and sample documents you can download, as well as useful identity theft links. More information is available from your local police and the agencies themselves.

1. Contact the police

Contacting the police allows them to start investigating the crime. You will also want to obtain a copy of the police report, the police report number, and the name of the investigator. Banks, credit card companies, and other agencies may require this information as proof of a crime.

When filing a police report, provide as much documentation as you can to prove you have been a victim of identity theft. Documentation including collection letters, credit reports, and an Identity Theft Affidavit can help the police create a thorough report.

If the identity theft occurred while you were away from home, you may also need to file a police report in the jurisdiction where the theft actually occurred.

Get a copy of the police report to submit to your creditors and others that may require proof of a crime.

Be persistent if necessary. You may be told they cannot provide a report. Be sure to let the police know that you need a report to provide to other agencies in order to resolve the identity dispute. If your local police will not file a report, contact the county and state police. You may also ask that they file a Miscellaneous Incident Report instead.

2. Contact the credit bureaus

Notify the three major credit bureaus (Equifax, Experian, Trans Union) that you have been a victim of identity theft and request that your file be flagged with a "Fraud Alert." Fraud Alerts expire after six months, so you may want to ask how you can extend it if needed.

Request copies of your credit report from each bureau to review. If information contained within your report is inaccurate, you may dispute it and request that it be changed.

Request your credit report again in a few months. This will help you confirm that the requested changes have been made and whether your report has been changed without your knowledge. This may also identify additional occurrences of identity theft.

EQUIFAX

Order Credit Report: (800) 685-1111

Report Fraud: (800) 525-6285

www.equifax.com

EXPERIAN

Order Credit Report: (888) 397-3742

Report Fraud: (888) 397-3742

www.experian.com

TRANS UNION

Order Credit Report: (800) 888-4213

Report Fraud: (800) 680-7289

Fax: (814) 447-6034

www.transunion.com

You may also want to file a "Victim Statement" with the bureaus asking them to notify you before any new accounts are opened or any existing accounts are changed in your name. This may reveal illicit attempts to open additional accounts in your name.

3. Close Suspect Accounts

Close the accounts you know or suspect involve identity fraud.

Checks: If your checks have been stolen or you suspect they have been misused, contact your financial institution to stop payments. Familiarize yourself with your state's laws concerning stolen and forged checks. You can contact your State Attorney General's office or local consumer protection agency to find out about any laws in your state related to identity fraud. Most states hold the financial institution responsible for losses related to a forged check. However, it may be your responsibility to notify the financial institution of the possible forgery in a timely manner.

You may also want to contact the major check verification companies directly. These companies can alert retailers who use their databases not to accept your checks:

Telecheck: (800) 710-9898

Certegy, Inc: (800) 437-5120

You can also find out if the thief has been passing bad checks on your account by calling SCAN at (800) 262-7771.

Credit Accounts and ATM Cards:

Report the incident to all institutions with which you hold credit card and ATM cards. Ask the financial institution or agency to send you a fraud dispute form to complete. When reopening new accounts, be sure to use new PINs to reduce the risk of future identity theft.

If your financial institution is not assisting you with the issues related to your identity theft, you may contact the agency with jurisdiction over your financial institution. If you are not sure what agency has jurisdiction over your particular financial institution, you can find out by visiting www.ffiec.gov/enforcement.htm.

If you suspect your investment or brokerage accounts have been altered without your permission, report it to the Securities and Exchange Commission. You can file a report using their online Complaint Center at www.sec.gov/complaint.shtml. Keep in mind that each creditor may have its own process for handling a case of identity theft. Therefore, be sure to specifically ask each creditor what its process is, what is expected of you, and what you can expect from them.

4. Contact the authorities

Federal Trade Commission

FTC counselors can take your report and provide additional advice on how to proceed if you believe you may have been a victim of identity theft. Their website is full of tips and also provides information on how to learn about laws in your state pertaining to identity theft. Also review, "[Take Charge: Fighting Back Against Identity Theft](#)".

Federal Trade Commission

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, D.C. 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

Social Security Administration

The SSA Office of the Inspector General investigates allegations of identity theft. If you know or suspect your SSN may be involved in the identity theft against you, you may want to contact the SSA to notify them, and to request a copy of your Social Security statement.

Social Security Administration

SSA Fraud Hotline
P.O. Box 17768
Baltimore, MD 21235
(800) 269-0271
Email: oig.hotline@ssa.gov

U.S. Postal Inspection Service

The USPIS is the law enforcement entity of the U.S. Postal Service and is the entity that investigates identity theft - specifically when the identity theft involves stolen mail or other violations of the integrity of the mail service.

U.S. Postal Inspection Service

475 L'Enfant Plaza, S.W.
Washington, D.C. 20260
(800) 372-8347
www.usps.gov/websites/depart/inspect

Federal Bureau of Investigation
FBI Internet Fraud Complaint Center
www.fbi.gov

5. Keep a Record of Your Actions

Keep a file of documents related to the identity theft. You will want to include documents such as disputed bills, credit reports, police reports, and any correspondence.

Maintain a record of your telephone conversations with the persons and agencies you contact for assistance. Be sure to record the date and time of the call, the name and title of the person you spoke with, and the things you discussed.

Follow up all telephone conversations in writing and send these letters certified with return receipts requested; maintain copies of these written correspondences for your file.

Maintain copies of any written correspondence you exchange related to the identity theft.

Keep original documents for your file; only mail copies.

6. Additional Fraud Resources

NON-PROFIT ORGANIZATIONS:

Identity Theft Resource Center

P.O. Box 26833
San Diego, CA 92196
(858) 693-7935
Email: voices123@att.net
www.idtheftcenter.org

Privacy Rights Clearinghouse

3100 5th Avenue
Suite B
San Diego, CA 92103
(619) 298-3396
Email: prc@privacyrights.org
www.privacyrights.org

STATE AND LOCAL GOVERNMENT AGENCIES:

Contact your State Attorney General's office or local consumer protection agency to find out whether your state has laws related to identity theft.

How do I protect myself?

Consider whether the company would be likely to ask you for the kind of information being requested. If you are at all in doubt about the authenticity of the communication, contact the company through familiar communication channels (e.g., the phone number provided on account statement).

Do not click on a link in an email when you are not sure of its legitimacy, even if it looks genuine. If you are at all in doubt, contact the company directly.

Avoid emailing personal and financial information.

Never open email attachments from unknown sources.

If Regularly review your account statements.

Do not share IDs/user names and passwords.

Change your passwords regularly.

Be aware that other Internet companies that you do business with may be phished.

If you pay an online service and/or have your credit card on file with an Internet based company, be cautious of emails from such companies that request you validate your credit card or checking account numbers.

Install the latest anti-virus and firewall applications to your computer.

Follow your computer manufacturer's recommendations to ensure that your computer is current on its patches. Refer to your computer's documentation or user's manual for further information.

Where do I find more information on how to protect my personal and financial data?

The Federal Trade Commission provides useful resources:

"How Not to Get Hooked by the 'Phishing' Scam", available on the Federal Trade Commission website at www.ftc.gov

"Take Charge: Fighting Back Against Identity Theft", available on the Federal Trade Commission website at www.ftc.gov

It is strongly recommended that you file a report at www.fbi.gov, www.ftc.gov or www.antiphishing.org.