Keeping Our Customers Safe

Intelletrace is committed to providing innovative, high-quality internet communications solutions that offer enhanced functionality over traditional telephone services at significantly less cost to the customer. In addition to outstanding quality of service, Intelletrace places a high value on the security and protection of our customers. We want to make sure you are informed and empowered on how to use technology, including the potential challenges that could arise around identity theft.

What you should know about identity theft

Identity theft occurs when someone uses another person's personal information (e.g., name, Social Security number, credit card number, passport), without the person's knowledge or permission, to commit fraud or other crimes.

Identity thieves use a variety of methods to steal your information. One of the most popular ways that thieves steal your personal information is through a scam called phishing. A phishing scam begins with an e-mail to potential victims that appears to come from a legitimate business, such as a bank or a phone company. The message may even be so bold as to suggest the company has experienced a security breach and they need to verify your account with your most current information. These types of requests will ask you to submit very sensitive information like credit card numbers, Social Security numbers, bank account information, or other personal data under a false pretense. The scammer's e-mail may even include a link to a legitimate looking Web site to capture this information.

How to protect yourself against identity theft – Deter, Detect, Defend

Deter
Deter identity thieves by safeguarding your information.

- Shred financial documents and paperwork with personal information before you discard them.
- Protect your Social Security number. Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give it out only if absolutely necessary or ask to use another identifier.
- Don't give out personal information on the phone, through the mail, or over the Internet unless you have initiated the contact and know who you are dealing with.
- Never click on links sent in unsolicited emails; instead, type in a Web address you know. Use firewalls, anti-spyware, and anti-virus software to protect your home computer; keep them up-to-date. Visit OnGuardOnline.gov for more information.
- Don't use an obvious password like your birth date, your mother's maiden name, or the last four digits of your Social Security number.
- Keep your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house.

Detect
Detect suspicious activity by routinely monitoring your financial accounts and billing statements.

Be alert to signs that require immediate attention:

- Mail or bills that do not arrive as expected
- Unexpected credit cards or account statements
- Denials of credit for no apparent reason
- Calls or letters about purchases you did not make

Inspect:

- **Your credit report.** Credit reports have information about you, including what accounts you have and your bill paying history.
    - The law requires the major nationwide consumer reporting companies—Equifax, Experian, and TransUnion—to give you a free copy of your credit report each year if you ask for it.
    - Visit www.AnnualCreditReport.com or call 1-877-322-8228, a service created by these three companies, to order your free credit reports each year. You also can write:
      Annual Credit Report Request Service
      P.O. Box 8.55281
      Atlanta, GA 30348-5281
- **Your financial statements.** Review financial accounts and billing statements regularly, looking for charges you did not make.

Defend

Defend against identity theft as soon as you suspect a problem.

- **Place a "Fraud Alert" on your credit reports, and review the reports carefully.** The alert tells creditors to follow certain procedures before they open new accounts in your name or make certain changes to your existing accounts. The three nationwide consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert; a call to one company is sufficient:
    - **Equifax:** 1-800-525-6285
    - **Experian:** 1-888-EXPERIAN (397-3742)
    - **TransUnion:** 1-800-680-7289

Placing a fraud alert entitles you to free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain.

- **Close accounts**. Close any accounts that have been tampered with or established fraudulently.
    - Call the security or fraud departments of each company where an account was opened or changed without your okay. Follow up in writing, with copies of supporting documents.
    - Use the ID Theft Affidavit at ftc.gov/idtheft to support your written statement.
    - Ask for written verification that the disputed account has been closed and the fraudulent debts discharged.
    - Keep copies of documents and records of your conversations about the theft.
- **File a police report**. File a report with law enforcement officials to help you with creditors who may want proof of the crime.
- **Report your complaint to the Federal Trade Commission**. Your report helps law enforcement officials across the country in their investigations.
    - Online: ftc.gov/idtheft
    - By phone: **1-877-ID-THEFT** (438-4338) or TTY, 1-866-653-4261
    - By mail: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580