

PRIVACY AND SAFEGUARDING POLICY

Privacy and Personally Identifiable Information

The tax industry is one that relies on clients sharing highly confidential information to accomplish the task of responding to a federal, state and/or other financial entities reporting requirements. Tax data is the rawest form of information that consists of social security numbers, financial account information, dates of birth, legal statuses, etc. This type of data is referred to as Personally Identifiable Information (PII) and is not readily known to or by the public.

Sharing PII can lead to potential interception with a purpose of unscrupulous intent when the data is transmitted digitally via unsecure means (e.g. email accounts and general webpages). It is expressly stated that emails from personal accounts (i.e. Yahoo mail, Google mail, Hotmail, Outlook, AOL, etc.) are often not secure, meaning they can be intercepted or read by others.

Working to Ensure your Privacy

CAF Enterprises USA Co. (the Company) has a duty to establish processes and protocols that will aid in protecting our clients' data. To protect this form of personal information from unauthorized access, we use security measures that comply with federal law. These measures include computer password and access safeguards, and restricted access to physical files. Access to private data is limited to employees of the Company utilizing a 'need to know' policy.

Computer and Hardware Processes

Based on business partner (i.e. Tax software provider, partner bank, secure storage host) requirements, the Company will:

- Utilize a software and/or router firewall when online and transmitting client data,
- Keep all antivirus software up to date, and

- Employ a combination of complex and expiring passwords to protect wireless networks, software and online account logins.

Physical Files and Mailing Process

- Physical files and check stock will be maintained in locking file cabinets or secured locations when not in use.
- Unassuming First-Class mailers, USPS priority mailing envelopes, or tinted waterproof vinyl mailer packets will be utilized to aid in privacy and ensuring the contents of the mailing are not revealed.
- Outgoing mail containing PII will be secured until delivered to a USPS receptacle or a Post Office.
- The Company will regularly monitor its mail receptacle during the tax season (January – May) for incoming client data and will immediately secure received items.
- Hardcopies of obsolete files will be destroyed onsite by the Company or professional destroyed by a licensed and bonded document shredding contractor.

Client Responsibility

The client also has a duty. When at all possible,

- Do not provide your date of birth, full social security number (SSN), credit card numbers, full bank account numbers, personal identification numbers (PIN), or passwords to anyone not permitted via phone, email or other forms.
- Do not provide your PII unless you have initiated the contact and know the person or company to whom it is being given.
- Do not provide your PII to anyone while in a public place or online on a public wireless network (WiFi) such as those found in airports, doctor's offices, hotels, fast food facilities or coffee shops.
- Store hard copies of your PII files in a secure location or a lockbox.

Other Contact and Processes

You are discouraged from submitting sensitive information via email means to the Company, however, if you must, CAFe will immediately save the email to a local archive drive before deleting the correspondence from its company inbox and deleted/trash email folders. We encourage the sender to do the same on his/her email account to ensure such data is not available in the event the email account becomes compromised.

Emails sent by CAFe will deliver PII in password-protected files. We will attempt to use PDF files with a minimum of 256bit encryption when possible. Passwords will be distributed separately or will be based on keys known by the recipient.

Most Company email correspondence and email footers will include the following (or similar) confidentiality and or security notice as a reminder to the recipient.

SECURITY NOTE

- For your protection (name, address, SSN), the attached copy of your return has been secured and can be opened only by using a proper password.
- For added security, you may wish to print and then delete or locally archive any attachment(s) containing personally identifiable data from your online email account. This will ensure your information is not compromised due to any successful hacking of your email account.
- CAF Enterprises will delete or locally archive tax return information from its active email account (in box/sent folder) within 2 days of the communication.

With or without the following disclaimer:

CONFIDENTIALITY/INTENDED RECIPIENT: *This e-mail, including attachments, may include confidential and/or proprietary information, and may be used only by the person or entity to which it is addressed. If the reader of this e-mail is not the intended recipient or his or her authorized agent, the reader is hereby notified that any dissemination, distribution or copying of this e-mail is prohibited. If you have received this e-mail in error, please notify the sender immediately by replying to this message or calling 804-224-2046 and delete this e-mail and any attachments.*

Information Collection, Use, and Sharing

The Company will not disclose PII to anyone who does not have a need to know right to the data. If presented with a valid court order, the Company will inform the client and proceed with complying with such order.

Your information will only be used in fulfilling your tax and financial assistance needs. We will not share your information with any third party outside of our organization, other than as necessary to fulfill your request (e.g. partner bank products, phone dial-in return status lookup, audit warranty company or additional financial services).

Unless you ask us not to, we may contact you via email and USPS mail in the future to inform you of Company specials, new products or services, or changes to this privacy policy.

Opting out

You may opt out of any future contacts from us at any time by contacting us via the email address or phone number given on our website.

Our Commitment

No industry is safe from security breaches; however, the Company will take adequate precautions to secure and protect your information. If a security breach occurs, we will notify you, the IRS, State tax administration and local law enforcement (as applicable) and work to mitigate client exposures to the best of our ability.

Contact Us

If you believe your information has been compromised or if you have questions regarding any transaction, please contact us immediately at: **804-224-2046** or via email at: cafenterprises@outlook.com. The Company will review the issue and if there has been a breach of our processes, we will move to limit your exposure and keep you informed of the process.