TWO-WAY STRONG

PRIVACY POLICY

The Two-way Strong Privacy Policy is an agreement between the operator of the Two-way Strong system (the “software producer”) and you (the “end user”). This privacy policy applies to the Two-way Strong User Account (“User Account”) and all data collected, stored, and processed in the Two-way Strong Web application (“Web software product”), the Two-way Strong User Authenticator (“Authenticator software product”), the Two-way Strong Budget Manager (“Manager software product”), and the Two-way Strong Merchant Register (“Merchant software product”). All of the software products where applicable are referred to as “software products”.

BY USING ANY ONE OR ALL OF THE SOFTWARE PRODUCTS AND THE USER ACCOUNT, THE END USER ACCEPTS THESE TERMS AND CONDITIONS REGARDING PERSONAL PRIVACY.

1. INFORMATION SECURITY.

The software producer provides protection and safeguards as technically practicable and in line with information security best practices to ensure confidentiality, integrity, and availability of data associated with the end user. Information security consists of multiple layers of controls and procedures that cover the computer network, data storage, software functionality, and data center operation.

2. RESPONSIBILITY FOR INFORMATION SECURITY.

There may be additional responsibilities, but this section communicates the most relevant ones regarding personal privacy.

a. Responsibility of the Software Producer.

The software producer protects the end user’s data with encryption as it is transmitted across the computer network to and from the end user’s computer. The software producer also protects the end user’s stored data in the database of the remote data center with encryption.

In any event of a security breach, the software producer will notify all affected end users and issue guidelines to take appropriate actions. The software producer will resolve any security breach in a prompt and expeditious manner. Depending on the severity of the security breach, software products may be temporarily offline and inaccessible.

b. Responsibility of the End User.

The end user protects their computer device against viruses and other threats by using an anti-virus software application. The end user follows commonsense practices to physically protect their computer device against damage, loss, or theft. In any event of a security breach or in any case where the end user’s computer device is damaged, lost, or stolen, the end user needs to notify the software producer. The software producer

can temporarily suspend the end user's User Account so that any unauthorized user will not be able use any software products in a fraudulent manner.

3. TYPES OF INFORMATION.

a. Unique User Name Identifier.

Each User Account is created with a unique user name that is defined by the end user at the time of user registration. The user name is not the end user's legal name. The end user can be creative to define a user name that obscures their identity. The unique user name identifier cannot be modified after user registration.

b. Personal Information.

The end user's personal information consists of legal name, home address, home city, home zip code or postal code, home country, phone number, e-mail address, date of birth, and two forms of government identification numbers. The software products require at least the end user's legal name, home address, home city, home country, and home phone number. All other personal data are not required.

c. Business Information.

If the end user is a merchant, the end user's business information consists of organization type, organization name, alternate organization name such as DBA, business address, business city, business zip code or postal code, business country, business phone number, business e-mail address, business website address, two forms of government identification numbers, industry sector and sub sector categorization names and classification codes, business and product descriptions, and names of primary and secondary products. The software products require at least the merchant end user's organization type, organization name, business address, business city, business zip code or postal code, business country, business phone number, one form of government identification number, industry sector name, business description, product description, and primary product name.

Submitted business information must match one or more legal documents that resulted in registering the business with a government agency. The software producer will review the new business entry against one or more legal documents submitted by the end user. If business information does not match one or more legal documents, the business will not be approved and the merchant end user will not be approved to sell and market their products and/or services in the software products.

Business information may be associated with one or more end users. For example, all of the employees can be registered and associated with the same business information. An existing end user, who had registered in the past and has recently been hired by the business, can have their User

Account updated to show their relationship to the business. If an end user had left the business or is no longer associated with the business, the end user's User Account can be updated to remove the relationship.

d. Location Information.

The Authenticator software product has GPS functionality to detect and capture the end user's present location. The Merchant software product also has GPS functionality to detect and capture the merchant end user's present location. The captured GPS coordinate point is associated with the date of capture and saved. The end user may have one or more GPS coordinate points that show where the end user has been. The purpose of capturing and storing GPS coordinates is part of the verification process in the software products to protect the end user against a potentially fraudulent activity. Several GPS coordinate points analyzed in combination provide a robust sample to identify fraud.

e. Financial Information.

As end users interact in sending and receiving payments and processing sales orders related to the purchase of merchants' products, the software products generate, process, and store financial information. Financial information consists of transaction identifier, date of transaction, transaction/payment type, transaction/payment status, payer identifier, payee identifier, brief description, total amount, transaction code, error code, total deposit, total withdrawal, and net balance. Financial information is further associated with sales order information that includes an enumerated list of products purchased and a breakdown of amounts listing sub amount, shipping, tax, total amount, and return change.

At the time of submitting a payment in the Web software product or in the Manager software product, the end user is required to select a payee, who is another end user, enter a brief description about the payment, and enter a total amount value. In interacting with a merchant end user in a physical location, the consumer end user sends their user name identifier and legal name from the Manager software product to the Merchant software product in an electronic wireless communication that is a few centimeters apart. In both cases, the end user takes an explicit action by clicking on a button or tapping the screen to send their user name identifier and legal name to process a payment.

The end user may schedule a payment for processing on a specified date in the future. The end user can edit the content of the scheduled payment up to the date of payment processing. Once the scheduled payment has been submitted for processing, the end user can no longer make any modification.

Once a payment has been submitted for processing, financial information cannot be changed by any end user. The complete financial information is generated by the computer and presented in a read-only format. The

processed financial information becomes a permanent record that cannot be modified.

f. Credit/Debit Card Information.

I. General Case.

In all cases where payments are sent and received to and from end users, the software products do not require the collection and storage of credit/debit card information. If the end user uses the software products to make payments, the end user does not have to store any copy of their credit/debit card number and other credit/debit card details in their computer device.

II. Exceptional Case.

The end user may choose to use their credit card or debit card to credit their user account with a deposit of funds drawn from the credit card or debit card. The end user may also transfer funds from their user account to their credit card or debit card. In either case, the Web software product does collect credit/debit card information for one-time use at the time of transaction. The Web software product will not store credit/debit card information. The end user must re-enter their credit/debit card number and other credit/debit card details each time the end user chooses to make a deposit or to transfer funds through the Web software product.

g. Bank Account Information.

The software products do not require the collection and storage of bank account information. If the end user uses the software products to make payments, the end user does not have to store any copy of their bank account number and other bank account details in their computer device.

h. Messaging Information.

One or more notification messages are associated with each payment transaction to show the communication record between the payer and the payee. Messaging information consists of a single message that contains subject, body or longer content, date of generation, sender, recipient, message type, message category, mode of transmission, transaction identifier, and scheduled transaction identifier. All messages are generated by the computer with subject and body pre-defined by the software producer and presented in a read-only format. The end user may add content by selecting from a pre-defined list and/or entering text. The end user’s input is appended to the pre-defined body and is indicated as user-submitted content. The end user is not required to submit additional content. Similar to the end result of financial information, messaging information becomes a permanent record that cannot be modified.

i. Product Information.

If the end user is a merchant, the end user can enter and store their product information in relation to their business. Product information consists of product identifier or product SKU, UPC barcode number, product name, product summary, regular unit price, discounted unit price, promotion code, promotion start date, promotion end date, and a public/private indicator mark. The merchant end user can enter one or more products in the Merchant software product. The Merchant software product requires at least product identifier, product name, product summary, regular price, and a public/private indicator. All other product data are not required.

j. Currency Information.

If the end user is a merchant, the end user can enter and store their currency information. Currency information consists of two currency codes and names, the exchange rate between the two currencies, the source of the exchange rate, the effective date of the exchange rate, and a public/private indicator mark. The merchant end user can enter one or more currency exchange rates for any number of currency combinations in the Merchant software product. The merchant end user may establish their own exchange rate independent of any official exchange rate published by a financial institution. The Merchant software product requires all currency information.

k. Information of Children Under the Age of 13.

The software products are designed for persons aged 13 and over. The software products do not collect the personal information of children aged 12 and under.

4. SHARING OF INFORMATION.

a. Personal Information.

Personal information is not shared with any third party organization that has not registered in the software products. The end user may have certain legal protections under applicable law. The end user’s legal name, full home address, and contact information may become available to an approved merchant to whom the end user had sent a payment. The end user gives their consent to be contacted by an approved merchant who is listed in the Payee list of the software products. If consent has been provided, the approved merchant may use the end user’s address and contact information to contact the end user about the merchant’s products and/or services. The number of approved merchants is limited to those who had received a payment in a past payment transaction. Any merchant who has not previously engaged with the end user cannot access the full address and contact information of the end user.

b. Business Information.

Business information is generally public information. Any registered end user may be able to review the business information of an approved merchant in the software products. The review of business information is limited to reading the content on screen in the end user's computer device. Another registered user cannot save displayed business information.

c. Location Information.

Location information is treated as private and confidential and will not be shared with any registered end user and any third party organization. The software products only use location information for internal verification purposes to detect and identify a potentially fraudulent activity.

d. Financial Information.

Financial information is treated as private and confidential and will not be shared with any registered end user and any third party organization. The end user may have certain legal protections under applicable law.

e. Messaging Information.

As it is tied to financial information, messaging information is treated as private and confidential and will not be shared with any third party organization and any registered end user other than the other end user who is associated in the payment transaction. Each notification message involves two registered end users. Only the two registered end users associated in the payment transaction are allowed to read the content of the notification message. The two registered end users can use the software products to read the content of the notification message.

f. Product Information.

A specific product that is marked as public may have its product information published in the software products. The merchant end user, who added the product information in the Merchant software product, can block publication or remove the product from further listing, by editing the product and marking the product as private. Only products marked as public are viewable to registered end users for browsing and purchasing. The merchant end user has the right to keep their product information private and inaccessible from other end users. Moreover, the merchant end user is the owner of the products that the merchant end user adds in the Merchant software product.

g. Currency Information.

Like product information, a specific currency exchange rate that is marked as public may have its currency information published in the software products. The merchant end user, who added the currency information in the Merchant software product, can block publication or remove the

currency exchange rate from further listing, by editing the exchange rate and marking the exchange rate as private. Only currency exchange rates marked as public are viewable to registered end users for browsing. The merchant end user has the right to keep their currency information private and inaccessible from other end users. Moreover, the merchant end user is the owner of the currency exchange rates that the merchant end user adds in the Merchant software product.

h. Scraping Information.

Technical controls are in place to disallow and block automated and anonymous search robots from accessing and indexing all the types of information. Third party websites and software applications are not allowed to scrape any type of information anonymously.

5. MANDETORY RELEASE OF INFORMATION.

The software producer may be mandated by applicable law or compelled by a law enforcement agency to release specific data records of one or more of the types of information. Any affected end user whose information needs to be released to government or law enforcement will be notified prior to release of any information. The end user will be given an opportunity to object to any release, and the software producer will forward the end user's objection to the law enforcement agency for review.

6. SELLING OF INFORMATION.

None of the types of information are sold to any third party organization.

7. EXPORTING INFORMATION.

The end user may choose to have their information exported into a format that can be used to import into a third party software application. The end user may choose this option to have an archived version of their information for storage in their computer device. The software producer may provide one or more data files containing all data records associated with the end user.

The end user must submit a request by e-mail in order for the software producer to begin the process of exporting information. The software producer will contact the end user to confirm the request and also to verify the end user. The request can be sent to the e-mail address, admin@2waystrong.com.

8. DELETION OF INFORMATION.

The end user may choose to close their user account and can have their personal information deleted. The end user must submit a request by e-mail in order for the software producer to begin the process of deleting personal information. The software producer will contact the end user to confirm the request and also to verify the end user. Any kind of data deletion must be requested in writing. The request can be sent to the e-mail address, admin@2waystrong.com.

9. OPT-OUT POLICY.

a. Exclusion from Location Tracking.

The end user may turn off or disable GPS functionality in their computer device to disallow the software products from detecting and capturing the end user's present location. Software products remain fully functional without GPS functionality.

b. Exclusion from being Contacted.

The end user indicates their consent to being contacted by an employee of the operator of the Two-way Strong software products or by an approved merchant by checking two boxes presented at the time of user registration. The checkboxes as indicators are available to the end user in the Manager software product. The end user may uncheck the checkboxes at any time to remove themselves from being contacted.

c. Exclusion of Product Information from Publication.

The merchant end user indicates their consent to publishing their product information by marking the products as public. The merchant end user may change the mark to private at any time to remove a specific product from being listed and viewed by other end users.

d. Exclusion of Currency Information from Publication.

The merchant end user indicates their consent to publishing their currency information by marking the currency exchange rates as public. The merchant end user may change the mark to private at any time to remove a specific currency exchange rate from being listed and viewed by other end users.

e. Other Opt-out Request.

For any specific opt-out request or if there are any concerns or issues, the end user may send an e-mail to the e-mail address, admin@2waystrong.com.

10. ABUSE AND BREACH OF PERSONAL PRIVACY.

In any event that personally identifiable information has been compromised, breached, or abused, either the software producer or the end user needs to provide timely notification of the occurrence. The end user can send an e-mail to admin@2waystrong.com The software producer will send an e-mail to the end user's e-mail address or contact the end user by phone. The software producer will investigate the matter and resolve it in a timely manner.

11. NOTIFICATION OF CHANGES AND ACCESS TO THE PRIVACY POLICY.

a. Subject to Change.

The Privacy Policy may be revised from time to time, as directed by

software revisions and/or internal organizational procedures. External events that impact business and/or industry or arise from laws, regulations, and/or legal actions may cause the Privacy Policy to be revised.

b. Notification of Change.

All end users shall be notified of any change to the Privacy Policy. A notification will be sent and is viewable in the Notification section of the software products.

c. Access to the Privacy Policy.

The latest version of the Privacy Policy can be downloaded from the Web at the following address: https://www.2waystrong.com/Pub/Doc. This Web page and any downloadable files listed therein are publicly accessible and may be found via search engines on the Web. The end user can also download the latest version from within the Authenticator software product.

d. Revision Date.

The Privacy Policy provides a revision date at the end of the document. If previous copies of the Privacy Policy had been saved in a local computer, the end user should check the revision date to be sure that the latest copy is being read. The latest Privacy Policy supersedes all previous versions.

Two-way Strong Privacy Policy

Dated: 05 April 2020