Online Banking Security Policy

As part of its commitment to its customers, AMPLIFY is committed to offering electronic access to its banking products and services in an efficient and secure way.

For this purpose, it relies on safety measures oriented to protect the privacy and the integrity of the personal and financial information that it handles; these measures include the interaction of the customer with AMPLIFY from the time the session is initiated until it is terminated.

Online and Mobile Banking Service

1. In order to use AMPLIFY's Online Service, the URL www.goamplify.com must be accessed. In order to use AMPLIFY'S Mobile Service, you must use our iOS or Android app available for download in the Apple App Store and Google Play Store. Our Mobile Service is also available for use on any mobile device which supports a mobile browser.

2. In order to perform the transactions required by the Online and Mobile Banking users, the credentials must be entered, which consist of a Login ID and a Password. You can enroll in Online and Mobile Banking Services by selecting the Enroll Now option at www.goamplify.com.

   Every time a new Password is delivered, it must be obligatory changed the next time the session is started.

3. The Password, which consists of a minimum and maximum number of characters, is a series of characters known only by the user of Online and Mobile Banking. In addition to minimum and maximum character values, our password policy also requires the use of at least one upper-case character, at least one special character, and at least one number.

4. For the purposes of guaranteeing the proper access of the users to the Online and Mobile banking service, some validations such as the following are performed:

   - Login IDs are locked after repeated unsuccessful attempts to register the login credentials correctly (Login ID and Password). In this case, you should contact AMPLIFY by visiting your nearest branch or by phone so that your password can be enabled.

   - Denial of reuse of a previously used password.

5. For security reasons, the Online and Mobile Banking service expires automatically after a period of time in which the computer or mobile device of the user remains

inactive. In the screen will appear an explanatory message that will require restarting the session.

6. In the event you forget your password, you must utilize the Forgot Password feature on the login page on our website or use the Forgot Password feature in our mobile app.

7. The Online and Mobile banking service is subject to periodic revisions and monitoring in order to detect attempts of attacks to the service.

8. AMPLIFY does NOT request updates of the confidential information of its customers such as: password or social security number.

Confidentiality of the Information

1. In order to guarantee the authentication, certification and encryption of the electronic transactions, AMPLIFY uses Digital Certificates which are represented by two components: a padlock closed in the bottom of the screen, which indicates that it is operating in a safe mode; and the Internet address (URL) that begins with “https” instead of “HTTP”.

2. AMPLIFY uses technological resources to protect and limit the non-authorized use of your Online Banking Service.

3. AMPLIFY relies on the services of permanent monitoring on the use of the illegal access of its trademark as well as of virus protection.

4. To guarantee the confidentiality and integrity of the information, AMPLIFY uses additional elements that will allow the validation of the identification of the users’ identity.

Responsibility of the Users of Online and Mobile Banking

1. To choose a strong password that is difficult to decipher by third parties, and which only is known by the authorized user. Some considerations are:

    - Do not to include user’s name as part of the login ID or password.
    - Do not to use key dates or information from private life, relatives, children, or professional life such as dates of birth, wedding, beginning of work, etc.
    - Do not to include personal or work telephone numbers.

Online Banking Security Policy

2. To protect the device with an updated antivirus that allows detecting and fighting malicious programs.

3. To maintain the confidentiality of the password, to avoid to write it in any place or unsafe means or within the reach of other people.

4. To immediately change the password whenever you suspect that it could have been exposed to:

    - Someone that could have seen it.
    - When you suspect or are certain that someone else (family, fellow worker, etc.) knows the password.
    - If you have not use it for more than 30 days.

5. To make sure to that you have logged out correctly from Online Banking after finishing using the services.

6. To change the password whenever the system asks for it or is considered advisable.

7. NOT to store credentials in the browsers.

8. To monitor your accounts and the historical detail of the historical transactions.

Reservations of AMPLIFY

1. AMPLIFY reserves the right to block the access to the users that have provided false information or for any other security reason.

2. AMPLIFY reserves the right to make changes, modifications or updates of these Policies at its sole discretion.