Quick Reference: Security

Overview

Consumer safety and security is our priority. By nature, we know credit and debit cards can be insecure, requiring only a signature or PIN number, used repeatedly and easily accessible by multiple sources. And there is no way to securely enter a PIN for online transactions.

We're raising the bar on traditional payments security measures by empowering our users with new, more stringent controls and options that prevent transactions from being processed without device authentication and user authorization. In short, we offer our users better protection for their hard earned money.

Key Security Features

- **Secure Platform** – Quick, easy setting controls to lock and unlock accounts putting complete control in the hands of the user rendering an unauthorized accessed PIN useless
  - ◊ User controlled access via Web, smart phone, SMS text and/or IVR

- **Mobile Authentication – mAUTH** is an added layer of security proactively requiring verification of all attempts – both authorized and unauthorized - at the time of the attempt
  - ◊ By default, each withdrawal of funds requires verification
  - ◊ The Integrated Voice Response (IVR) system calls the mobile number tied to the mobile monē account, requiring either voice identification and verification or SMS text verification for successful completion
  - ◊ Unauthorized attempts are thwarted and can be reported

- **Real-time Notification** – Automated notices by email, SMS, IVR or any combination, keeps the user up-to-date at the moment of activity and potential impact
  - ◊ Automated notices are available for deposit, withdrawal, purchase authorization, settlement, attempted use when locked, low balance and funds redemption

- **Personal Financial Firewall™ (PFF)** – A secure FDIC insured funds safety zone designed to support deposits and authenticated transfers only

- **Cellular Account Verification** – Automated verification the registered mobile number belongs to the mobile monē account

- **Real-time PIN Management** – Easy change of PIN anytime and single use PIN assignment

HIGHLIGHTS

- Users stop exposing 16 digit card numbers and account information by protecting their information behind the mobile phone number associated with their individually FDIC insured mobile monē account
- Users store funds in a completely secure mobile monē Wallet, which can be locked and unlocked anytime
- Users easily move funds to and from their linked MasterCard® Prepaid Debit Card at any time
- User's MasterCard® Prepaid Debit Card can be locked and unlocked at any time
- Secure account activation and deactivation with multi-factor authentication and authorization
- Regulatory compliance with EFTA, CCD/KYC, U.S. Patriot's Act; meets industry standards for maintaining security and privacy for sensitive user data (Payments Card Industry – PCI)
- Comprehensive risk management monitors risk across entire user profile, not just the transaction level
- Multi-channel, secure access enables payments anytime, anyplace, anywhere

THE ESSENTIALS

Personal Financial Firewall™

Lock/Unlock Account


Device & Address Verification


Real-time Notifications & Transaction Authentication

THEFT vs. FRAUD

The impact of identity fraud can be time consuming, costly and negatively impact many different areas of a consumer's life. If fraud ever happens, work through your bank, credit union or protection services provider to report problems immediately and begin resolving the problem.

It's important to understand the difference between Identity Theft and Identity Fraud.

- *IDENTITY THEFT* is the exposure of a consumer's personal information and typically happens when a consumer's personal information is confiscated by another individual without their permission.
- *IDENTITY FRAUD* is the actual misuse of information for financial gain and occurs when criminals take illegally obtained personal information and make fraudulent purchases or withdrawals, create false accounts or modify existing ones, and/or attempt to obtain services such as employment or health care.

Personally identifiable information such as your Social Security Number (SSN), bank or credit card account numbers, passwords, telephone calling card numbers, birth date, name and address can be used by criminals to profit at your expense.

Your identity can be stolen in many different ways.

- Lost or stolen wallets
- Receipts from purchases made in a store
- Stolen information from your home or workplace by a family member, friend, or employee
- Computer Hacking and Spyware
- Stolen mail
- Data breach of records at a business
- "Dumpster diving"
- Fraud scams (email, phone or direct mail)
- "Shoulder surfing," (information obtained by looking over your shoulder)
- Social networking sites

What Thieves Might Do "As You"

Thieves typically use stolen information to commit financial identity fraud crimes and criminal and government fraud crimes:

- Access existing checking account to create false checks
- Change the information on an existing credit card, debit card or online bank account
- Open new credit or loan accounts
- Sign-up for new cable TV, Internet, Home phone, cellular phone or energy/utility service
- Obtain medical services
- Acquire a state issued Identification Card or Driver License
- File taxes or obtain a tax refund
- Give a false identity when arrested or to avoid paying tickets
- Give false identity to avoid paying IRS Liens or to gain employment
- Apply for Government services or benefits
- Rent an apartment or lease a car

eMONEco SOLUTION

Our platform comprehensively places total security control in the hands of the mobile monē account holder. This is achieved by a combination of several components working in harmony to deliver increased levels of security.

Full Protection - Block Theft and Fraud

1. A mobile monē account holder's personal information is never used in the processing of a transaction between an authorize merchant and a mobile monē account holder.
2. Funds are placed behind a 100% secure Personal Financial Firewall, that requires funds are unlocked for use, or moved into an authorized payments transaction zone for use.
3. Whether unlocked for use, or moved to an authorized payments transaction zone, the system authorizes the funds movement via a device authentication and account holder identity verification process.
4. Payment is successfully handled with complete end-to-end security by a simple SMS command.

While this method delivers complete security, given it requires the acceptance of eMONE merchant participation, we also enable our users the ability to function in the traditional standard environment and continue the delivery of the highest levels of security and protection. As such, if a merchant is not a part of the "eMONE" eco-system, we take a slightly different approach.

Protection - Limit Theft and Block Fraud

1. A mobile monē account holder's personal information is required to be used in the traditional payments process.
2. Funds are still placed behind a 100% secure Personal Financial Firewall, and moved to the mobile monē MasterCard® when needed.
3. The system authorizes the funds movement via a device authentication and account holder identity verification process.
4. The MasterCard® must be unlocked prior to payments use.
5. The MasterCard® payments instrument is further protected by our platform via a user definable PIN setting that can be changed as often as the user desires.
6. Payment is successfully handled with complete end-to-end security.

While all of these steps seem complex, the entire process is designed to be handled via two simple keystrokes or voice commands and in a very unique manner, can be controlled across multiple channels: voice, DTMF, SMS text, online or mobile application.