Paystar Remittance Suite
Tokenless Two-Factor Authentication
Introduction

Authentication is the process by which a computer system positively identifies a user. It is commonly considered to be one of the weakest links in modern computer security systems. Every day a new story emerges about identity theft or fraudulent transactions due to stolen credentials. With the proliferation of network-based and online applications, this trend is only going to continue. Unfortunately, the dominant authentication system in production today is based on user names and passwords. This relatively weak system is subject to a number of flaws, including notoriously poor user password choices, password harvesting via keylogging software, phishing, man-in-the-middle attacks and others.

The most common solution to these authentication problems is to use a two-factor authentication system. Two-factor authentication works by requiring both something the user has and something the user knows, as opposed to just something known (typically a password). The “something you have” is usually a piece of hardware that is impossible (or at least very difficult) to duplicate, and the “something you know” is typically a password or PIN (primary identification number). Two-factor authentication systems become secure because it is very difficult to obtain both factors. Even if an attacker manages to learn the user’s credentials, it is useless without also having physical possession of the authenticating device. Conversely, if the user happens to lose the physical device, the finder of that device is unable to use it unless (s)he can also provide the user’s password or PIN.

Security professionals deploy various two-factor solutions, but no solution has commercially displaced traditional user name and password authentication.

The industry has enterprise-wide deployments of token-based systems from vendors such as RSA® and VeriSign®, smartcard-based solutions, and various forms of biometric authentication. Each solution has significant drawbacks, historically leading to limited adoption by consumers due to the expense of maintaining such systems. For online consumer logins, such as banking and financial websites, these limiting factors have hampered two-factor deployments. Such websites have instead opted to deploy security questions and image identification (SiteKey™) as the additional layer of security.

Translink provides a strong, two-factor authentication service within its platform that requires no additional investment in physical devices or authentication servers. It uses the public telephone network for the second authentication factor, which allows Translink to employ a rapid and inexpensive solution while maintaining all the advantages of a two-factor authentication system.
Two-Factor Authentication

Translink has implemented two-factor authentication using the user's telephone as the second factor of authentication. The transfer or payment process begins as a normal transaction to the system, in which the user requests a transfer of funds or a purchase from their mobile phone, online website or within a brick-n-mortar merchant location. The system initiates a phone call to the user's registered phone number. The user then answers the phone and indicates whether or not to authenticate the transaction by entering their personal PIN. Once the user acknowledges the authentication attempt via the phone call, the system completes the pending transaction and the transaction proceeds as normal.

This authentication rests on its use of the user’s telephone as a second (physical) authentication factor. Telephones are extremely difficult to duplicate and phone numbers are extremely difficult to intercept. The combination of phone and a memorized password (PIN) yields the strong, two-factor authentication in a minimal hassle highly secure process to protect the user and his or her funds.

This architecture has a number of advantages over traditional two-factor systems. Most importantly, it doesn’t require the user to carry an extra physical device. It instead leverages a device the user carries already. Most users already have mobile phones (there are about 3.5 billion active mobile subscriptions today), and they’re going to carry them regardless. Most importantly, each one has a world-wide unique identifier that’s almost impossible to copy: the phone number.

In addition to the advantage of using an existing device, Translink employs the only two-factor authentication system in the world that allows for instant attack detection. Every transaction attempt in which the attacker knows the user’s information will generate a phone call to the (true) user. That user can immediately block the account and instantly notify Translink’s fraud department, who can instantly take appropriate action.
Using Our Two-Factor Authentication

The security of Translink’s solution lies in its ability to strongly authenticate users based on proof that they know a secret (their PIN) and are in physical possession of a unique physical device (their phone). While it may be possible (or even easy) for an attacker to gain access to a user’s credentials, it is usually a much more difficult problem to obtain that same user’s phone.

Password theft is rampant on the Internet. The proliferation of botnets and phishing sites means stolen credentials will probably be a fact of life for years to come. Translink neutralizes the threat of password theft, since phones are not vulnerable to being stolen in the same ways that passwords are.

Translink’s solution can be configured in either Standard Mode or PIN Mode. Standard Mode requires only that the user answer the phone and press a button to prove that the authentication is expected and approved. In PIN mode, users are required to enter a PIN that functions essentially as a third confirmation. This makes it even more difficult for an attacker that comes into possession of the user’s phone to finish the transaction. This PIN is never saved on the phone in logs since it is only a response to a received call. SMS factoring does not provide this same security and ingoing and outgoing SMS’s are saved in the phone’s history.

Translink’s solution can also be configured using either a user-supplied voice message (similar to recording a voice mail greeting) that only the legitimate Translink server could have, or by having the end user select a random authentication word for the Translink authentication server to repeat to the user at every authentication call. The latter system is similar to the SiteKey™ system in use by other financial websites.
Conclusion

Usernames, passwords, CVV’s simply no longer provide enough security in many environments today. With our extensive experience in managed security, Translink enables users to experience the benefits of strong authentication without placing undue burdens on them or on their budgets. For the first time Translink allows banks to provide two-factor authentication to anyone in the world, with a simple formula: something they know (their password - PIN) and something they have (their phone).