

# Remote Identity Confidence

## RemoteID™

Remote Device Authentication

Conventional approaches to multi-factor authentication require users to carry new hardware device and/or to install new software, often a cost-forbidden solution for mass-market internet applications such as online banking. RemoteID delivers a strong two-factor authentication solution that does not require additional hardware or software installation, therefore it can be deployed to millions of users instantaneously at a fraction of the cost of other hardware or software based authentication products.



### How It Works

When an online user accesses a website protected by RemoteID, their computer device will be remotely scanned by RemoteID. RemoteID then builds the fingerprint of the user's computer, and uses the fingerprint to authenticate the user. Combining the device's fingerprint with a user name and password, Web applications can restrict access to only trusted devices and authenticated users.

To combat against phishing attacks, Web Applications can combine RemoteID and SiteStamp, a simple and reliable site authentication solution, to create a strong, two-factor and two-way authentication system.



### Restore Consumer Confidence

The prosperity of e-commerce and e-banking is being undermined by user insecurity and overly complex security process, as a result of attempting to combat against the fast growing phishing attacks.

RemoteID and SiteStamp provide e-commerce and e-banking with a two-factor and two-way authentication solution that helps to restore customer confidence as the system does not compromise consumer usability or change the way users login and transact online. The solution is totally transparent and works as if it did not exist.



### Ideal for e-banking and e-commerce

RemoteID is designed to authenticate your customers, at logon and during transactions. Each computer device accessing your website is analysed by a remote fingerprinting mechanism that provides a real-time authentication and risk assessment on all activities. The authentication takes place behind the scenes and is invisible to the user. Suspicious computer devices or transactions can be further interrogated by deploying additional authentication channels.



### Key Benefits

- **Zero Footprint** - No need to install any software or hardware. The solution can be quickly deployed to a large user base.
- **User Friendly** - No need to change the existing login process. The two-factor authentication works in the background that is invisible to the user.
- **Low Cost** - No user education, no expensive deployment and maintenance.

