POLi Payments Security Summary

POLi Payments puts security at the forefront of all product development and infrastructure deployment. As a result we encourage customers and merchants to educate themselves about POLi including the robust security features that have been built into the POLi solution.

Security Features Highlights:

- Best practice in network, physical and application security has been adopted by POLi Payments.
- At each step within the transaction lifecycle the transaction details provided by the merchant are validated against those within the Internet Banking session to ensure they have not been altered. Furthermore, POLi will fail a transaction whenever validation fails ensuring transaction integrity.
- Customers will always be communicating with their bank and not a phishing site. This is achieved via certificate validation ensuring the certificates have not been revoked.
- Customer Internet Banking credentials are not captured or stored by POLi. Furthermore, no registration is required by a customer to use POLi.
- By implementing a distinct web-service call which occurs outside of the original transaction (the 'Nudge') merchants can be assured that the correct transaction outcome and details are communicated. This ensures that any attempt to hijack or tamper with the original transaction communications flow will not result in the merchant crediting a false transaction.

Security Assessment Review

To ensure that at no point merchant or customer details are compromised POLi 3 has been independently audited by Secutiy-Assessment.com. This audit was carried out in February 2012.

Security-Assessment.com is a solely dedicated, vendor neutral, ethical hacking security company in New Zealand who have now expanded into the Asia Pacific region; they are leaders in web application / penetration testing, architecture and technology assessments and overall Enterprise Security Management services, in addition to being a certified Payment Card Industry assessor.

This following is a summary of the security audit:

- Testing was carried out from the view of a malicious external user, and as an authenticated legitimate user. POLi Payments provided Security-Assessment.com the relevant user credentials to use during this security review.
- Application testing was conducted in a 'black box' manner, and Security-Assessment.com was not provided any technical details or detailed documentation regarding the project or environment.
- Review of the reverse proxy solution was conducted in a 'white box' manner, Security-Assessment.com was provided with full access to the application source code, and detailed documentation regarding the solution.

POLi Payments Security Summary

- The level of security implemented within the POLi Payments application was found to be comparable to industry standards and mostly conform to the OWASP (Open Web Application Security Project) developer guidelines.
- Security-Assessment.com was not able to perform any unwanted actions which might compromise the integrity of the applications. It was not possible to manipulate payment information or reuse transaction details to perform unauthorised transactions.
- The POLi Payments applications did not store, transmit, or reuse internet banking details during the initiation of transactions. It was not possible to gain access to internet banking credentials via any vulnerability or misconfiguration.
- Security-Assessment.com identified no vulnerabilities during the reverse proxy solution code review. The solution performs the necessary tasks without exposing banks or users to any security issues.
- The POLi Payments applications have implemented many Microsoft recommended security practices regarding .NET application development and deployment. Features such as Event and Request Validation were found to be enabled and functioning.
- Some issues identified within the applications which are categorised as Low (severity findings relate to housekeeping issues or configuration settings). No issues categorised as Critical, Urgent, Medium or Minor have been found. Remediation of these issues has been implemented.