MERCURY®

November 20, 2015

Smyth Retail Systems, Inc.
Tim Smyth
7100 Whipple Ave NW Suite D
North Canton, OH 44720
RE: **Smyth Retail Systems V5.0**, certified out of scope implementation using Mercury and Datacap System's dsiEMVUS® or dsiPDCX™, Mercury's E2E & Tokenization, Datacap's In-Store NETePay™ and the VeriFone® Vx805

Dear Mr. Smyth,

Smyth Retail Systems V5.0 has successfully completed the requirements for U.S. EMV certification with Mercury. This certification combines EMV transaction and receipt validation using the dsiEMVUS® or dsiPDCX™ and the VeriFone® Vx805 in a configuration supporting the added layered security of End to End encryption (E2E) and Tokenization (MToken). By successfully completing the Mercury certification, **Smyth Retail Systems** has met compliance and direct card brand EMV certification requirements.

Datacap's dsiEMVUS® enables EMV processing on the MercuryPay® platform. Mercury certified this processing path with each card brand directly, eliminating the requirement for ISVs who, in turn, complete the Mercury certification. The dsiEMVUS, in conjunction with the NETePay 5.06.10 isolates the POS from the payment transaction process and access to sensitive cardholder data. As a semi-integrated EMV solution supporting encryption and tokenization, it is out of scope of PA-DSS and the requirements of a direct EMV card brand certification.

Mercury's E2E solution removes developers or ISVs from scope because cardholder data is no longer present in the payment application. Exposure and risk to vulnerabilities is reduced or removed altogether. Security is increased because cardholder data is encrypted at the reader. Malware that scrapes active memory on a computer would not get clear text card data on transactions properly processed through the E2E devices.

Mercury's E2E solution works with industry leaders, such as VeriFone, in the manufacturing of E2E devices to securely encrypt cardholder data at the point of interaction and passes that data to Mercury for decryption and processing.
As a validated and listed Level 1 Service Provider, Mercury's CDE (Cardholder Data Environment) is reviewed under our QSA audit which includes thorough testing and analysis of our E2E decryption environment; given the E2E decryption environment handles cardholder data, this environment must be compliant with PCI DSS. Mercury's service provider listing is available at Visa's Global Registry of validated Service Providers, http://www.visa.com/splisting/, and MasterCard's SDP Program (Site Data Protection) of compliant Service providers http://www.mastercard.com/us/company/en/docs/SP_Post_List.pdf

- **Smyth Retail Systems V5.0** is certified using Mercury and Datacap System's dsiEMVUS or dsiPDCX with the use of DataCap's In-Store NETePay. Coalfire, an approved Qualified Security Assessor confirmed that Point of Sale (POS) applications which integrate to Datacap's NETePay with dsiEMVX or dsiPDCX may be removed from scope of PA-DSS compliance requirements.
- **Smyth Retail Systems V5.0** is certified using the VeriFone VX805, a PCI PTS approved PIN device. The validation can be confirmed on the PCI SSC's list of approved PTS devices, https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php.
- **Smyth Retail Systems V5.0** is certified using Mercury's E2E encryption and tokenization.
- **Smyth Retail Systems V5.0** is certified using Mercury as the EMV processing path to the Card Brands.

Because you have implemented these secure technologies, and because we understand how these technologies remove your point of sale device from the scope of storing, processing or transmitting cardholder data, Mercury considers this an acceptable payment application for merchants and demonstrates that our customers are going above and beyond to provide secure solutions protecting cardholder data. Mercury is pleased to board merchants using this solution to process with us. Encrypting the cardholder data at the point of swipe is a path to compliance that is meaningful, practical and trusted.

Sincerely,
Pam Galligan
VP Compliance and Industry Relations
compliance@mercurypay.com.

Please note that use of Mercury's E2E, tokenization and Hosted solutions do not remove the user from scope of PCI DSS security standards or the requirement and responsibility to comply with applicable PCI DSS. For more information, visit the PCI Security Standards Council website at https://www.pcisecuritystandards.org.