THE NILSON REPORT

FOR 46 YEARS, THE LEADING PUBLICATION COVERING PAYMENT SYSTEMS WORLDWIDE APRIL 2017 / ISSUE 1107

Mobile Wallet Security from Paygilant

Legacy mobile phone fraud fighting technologies operate within a network, as is the case with Visa and Mastercard, as well as on a card issuer's back-end processing platform where authorization requests are either approved or declined. Typically, these back-end systems fight mobile fraud using algorithms created to fight plastic card-based fraud. A fundamentally different approach is available from start-up Paygilant — on-device security.

Paygilant's risk engine and fraud detection product learns and maps the spending behavior of each wallet user and spots fraud on in-store (NFC and QR code-based) and in-app transactions as well as on person-to-person money transfers when they are in progress, before the authorization request is even sent to the issuer by the acquirer.

Its algorithm considers scores of parameters about a pending payment, including the historical buying habit of the cardholder, and it factors in any biometric (behavioral and physical) security that might be available.

The company's SDK is linked in the smartphone to the issuer's mobile payment app.

Protection is provided even when network connectivity doesn't exist back to the issuer as well as when purchases are automatically approved because a payment is below a daily or per-transaction price ceiling. A cardholder's map is updated on their smartphone every two or three days. There is no dependence on the issuer's back-end system.

Its SDK is linked in the smartphone to the issuer's mobile payment app.

Paygilant says its technology significantly reduces false positives for fraud, which saves the issuer money by not triggering a second authentication request such as a text message or call center contact and other related operational costs.

Paygilant's technology can review 100 times more transactions than typical back-end systems.

An added benefit of having fraud fighting data stored on the cardholder's handset is there is no conflict with privacy laws that prevail in some jurisdictions covering storage of consumer data at remote sites.

Paygilant's fraud fighting is predicated on the belief that systems are not balanced for risk, and require unnecessary friction in the checkout process. They require the use of a PIN or password for transactions that have little risk, despite the fact that PIN and password theft is already a proven skill of criminals. Their use does not guarantee a fraud-free transaction. Even physical biometrics such as fingerprints do not guarantee a fraud-free transaction. Criminals who steal valid payment card credentials can open a new account and use their own fingerprints on their own smartphones. This deceives issuers into assuming a valid cardholder is initiating a payment.

Paygilant launched four months ago. To prove claims for its on-device technology, Paygilant worked with Citi in the U.S. It tripled the fraud detection rate and gave the bank a return-on-investment calculator that

> see p. 2

Mobile Wallet Security from Paygilant

from page 1...

determined cost savings using Paygilant versus their existing back-end systems.

Paygilant is doing similar proof-of-concept tests with two banks in Italy and with mobile wallet providers in India and South Africa.

Paygilant holds patents in 12 countries. It has received financial backing from two fintech venture capital firms, Israel's largest bank, and a grant from the European Union. It also has strategic support from Visa.

Ziv Cohen is CEO at Paygilant in Tel Aviv, Israel, 972 (3) 522-1879, zivc@paygilant.com, www.paygilant.com.