One-Time Password Authentication is Standard Industry Practice, but Fraudsters Are on the Move: Auriemma Group

In the wake of frequent data breaches, one-time password (OTP) verification has rapidly replaced knowledge-based questions as the stepped-up authentication standard for the card industry. However, fraudsters are increasingly exploiting susceptibilities of OTP technology – either by hijacking one of the delivery channels to intercept the OTP message or leveraging social engineering tactics to trick customers into revealing passcodes.

NEW YORK (PRWEB) April 10, 2019 -- In the wake of frequent data breaches, one-time password (OTP) verification has rapidly replaced knowledge-based questions as the stepped-up authentication standard for the card industry. However, fraudsters are increasingly exploiting susceptibilities of OTP technology – either by hijacking one of the delivery channels to intercept the OTP message or leveraging social engineering tactics to trick customers into revealing passcodes.

OTP is a critical component of multi-factor authentication (MFA), providing an additional security layer on top of the conventional username and password combo. It typically involves a dynamic password sent to the customer’s registered mobile number or email address to verify identity.

The industry widely relies on OTP authentication, which has been effective according to data from Auriemma’s Card Fraud Control Roundtable – when an OTP is triggered, on average 8 out of 10 customers are able to authenticate successfully. Moreover, 77% of card issuers indicated that OTP technology was being utilized for enhanced authentication of risky monetary transactions (primarily high-dollar purchases), and 70% utilize OTP as an added verification step for questionable non-monetary transactions, such as adding a supplementary cardholder.

“Card issuers operate under the baseline assumption that usernames and passwords have been compromised in recent data breaches, making MFA a critical component of the customer’s authentication journey,” said Ira Goldman, Senior Director of Auriemma’s Fraud Control Roundtables. “Because of its widespread usage, fraudsters are looking for any perceived vulnerability to exploit within OTP verification.”

Indeed, OTP verification has some vulnerabilities. SMS and email are the predominant OTP delivery channels. With billions of email addresses compromised across several large-scale breaches, email is considered the riskier channel and its popularity has dropped, with only approximately 50% of issuers verifying OTP via email. And while SMS is being leveraged by all issuers, sophisticated fraudsters can still gain illegitimate access to SMS-based OTP via number porting and SIM swap tactics. Consequently, it is crucial to use sufficiently tenured mobile numbers along with third-party vetting to establish credibility prior to OTP delivery.

The latest challenge has been the uptick in fraudsters directly targeting customers to obtain the OTP. To achieve this, criminals impersonate a customer’s bank, issuer, or even law enforcement to trick them into disclosing the OTP. As a countermeasure, issuers are beefing up awareness campaigns warning customers about fraudsters’ tactics and steps to evade them.

In response to fraudsters’ increasing sophistication, lenders are currently exploring new verification tools that
involve greater utilization of biometrics e.g., voice and facial recognition, and passive authentication elements e.g., keystroke patterns and browsing speed. In addition to enhanced security, biometric authentication also alleviates the customer friction challenges that accompany OTP verification.

“Fraudsters continue to demonstrate sophistication and flexibility to overcome authentication hurdles, emphasizing the need for the industry to develop better mousetraps,” Goldman said.

About Auriemma Roundtables

Auriemma’s Card Fraud Control and Bank Fraud Control Roundtables provide members with access to industry expertise and best practices to stay ahead of fraud trends and improve fraud mitigation via actionable insights.

About Auriemma Group

Auriemma Group’s mission is to give clients access to data and intelligence that drive decision-making. We provide information and advisory services in four areas: co-brand partnerships, consumer research, corporate finance, and operational intelligence. Founded in 1984, Auriemma serves the consumer finance industry from our offices in New York City and London. For more information, visit us at www.auriemma.group or call Ira Goldman at (212) 323-7000.
Contact Information
Diana Middleton
Auriemma Group
http://www.auriemma.group
212-323-7000

Online Web 2.0 Version
You can read the online version of this press release here.