ERIK NASARENKO
VENTURA COUNTY DISTRICT ATTORNEY
NEWS RELEASE

Follow us @VenturaCountyDA
vcdistrictattorney.com

Contact: Joey Buttitta
Title: Communications Manager/PIO
Phone: (805) 767-3400
Email: Joey.Buttittta@ventura.org

Approved: SW
Date: January 2, 2024
Release No.: 24-001

New Year, New Fraud Warning About QR Codes
Tips to Avoid Becoming a Victim

VENTURA, Calif. – The Ventura County District Attorney's Office is informing the public about a recent report our office received from the International Association of Financial Crime Investigators (IAFCI, December 2023) regarding QR code fraud, and the relative financial and security risks associated with this increasing growing form of fraud.


Image 1

QR codes or "Quick Response codes" (see image 1) are barcodes that can be read (scanned) by an imaging device, such as a camera on a phone. When a QR code is imaged by a device, it can direct the device to perform functions such as opening websites. There are certain private and public entities that will use QR code applications to facilitate digital payments transactions for customers (scan and pay). QR codes can be placed or affixed anywhere, such as a physical location (a sticker on a store window) or non-stationary settings (advertisements on print or in digital format).

"As technology provides customers more options to quickly and easily conduct financial transactions, what sometimes follows right behind are the quick and easy methods criminals use in an attempt to steal from those very customers," said Investigator Richard Elias, a member of the Ventura County District Attorney's Office Major Fraud Division.

Certain criminals ("fraudsters") have taken advantage of the growing use of QR code technology to trick users into scanning illegitimate QR codes, which fraudsters can place or affix with relative ease anywhere. This can be as easy as placing a QR code sticker over a pre-existing QR code (see image 2). Once a victim accesses the malicious QR code, they are routed to a fraudulent website posing as the official site of what the customer intended to visit or

Image 2
(QR sticker over other QR code)

do business with. This could ultimately lead to financial losses or the later misuse of personal identification and financial information.

To prevent this, consumers are encouraged to:

1. Consider where and how QR codes are being displayed and if those displays reasonably correspond with the transactions being considered.
2. Before “clicking” to accept a scanned QR code, check the phone camera screen to see what website (URL address) is associated with that QR code (this should pop up when the phone scans the code).
3. After accepting a scanned QR code, check the website (URL address and site features) to make sure the website is associated with the legitimate company/entity it claims to represent. Discontinue or check with the entity directly if there are any doubts of authenticity.

If you have been a victim of QR code fraud, or suspect QR code fraud is taking place, please report the matter to your local law enforcement agency and immediately report any suspected financial fraud to your bank or credit card company.