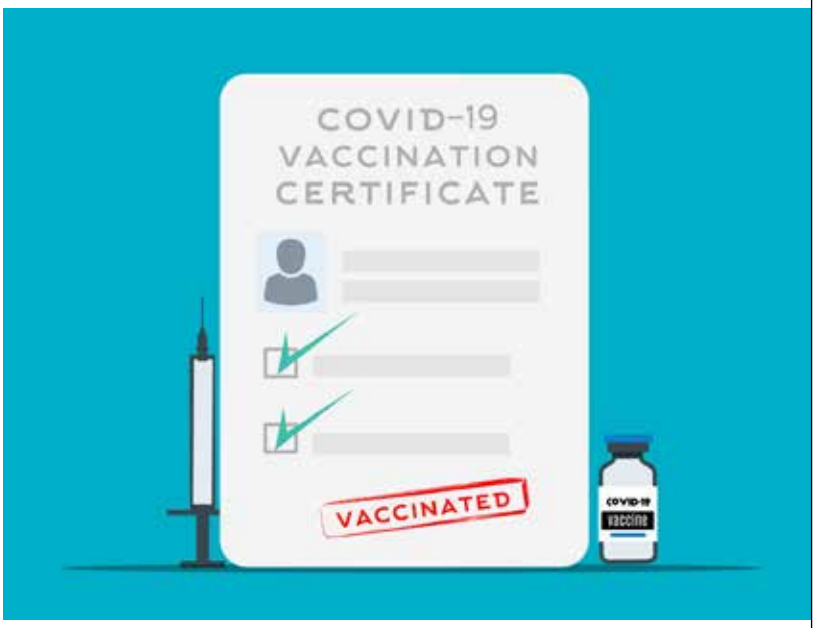
# COVID-19 FRAUDSTERS

**Dr Gareth Owenson** *reports on the rise of fake vaccine cards on the Dark Web*




**While political and social debate caused by the proposed use of COVID Vaccine Cards (CVCs) raged across traditional and social media platforms, underground networks of cybercriminals found new ways to exploit public fear and unease for financial and strategic gain.**

This article reviews some key findings from Searchlight Security's report, which investigates the dark web demand for CVCs by analysing listings on popular Dark Web markets. The result of analysis of over 3-million listings from more than 70 Dark Web markets posted between January 2020 and January 2022 help shape recommendations for policy makers and researchers on how to investigate and defend against this emerging threat from the digital underground.

The volume of CVC listings has increased significantly in the past year, with the total number growing on average by 186 percent per month. The lion's share of these originate from a single Dark Web marketplace, suggesting that despite international policing efforts, cybercriminal activity is flourishing. The most common price of a Dark Web CVC listing is $500 (£370). With a very low production cost for these cards, profit margins remain high for cybercriminals, with specific sellers beginning to corner the market from an early stage and set themselves up as key distributors.

Meanwhile, technological improvement to the way governments verify vaccination status, such as QR codes, hasn't stopped criminals from attempting to imitate them. Dark Web vendors were quick to respond, with digitised CVC listings appearing on markets as early as mid-2021. Some even claim to have sourced legitimate QR codes from medical staff, though this can't be independently verified.

When analysing cybercriminal activity, it is worth assessing what factors could be driving the actors involved,

**28 PERCENT OF DARK WEB CVC LISTINGS DIRECT BUYERS TO ENCRYPTED MESSAGING PLATFORMS LIKE WHATSAPP**

besides the obvious financial incentives. Many Dark Web vendors selling CVCs previously or subsequently advertised unrelated listings covering a wide range of goods and services, including illegal substances and stolen credentials. This supports the notion that existing sellers pivoted to meet the new demand for CVCs, as was the case for earlier pandemic-related products such as masks and purported COVID-19 treatments.

That said, recently there has been an increase in Dark Web market vendors exclusively focused on the sale of CVCs. Perhaps unsurprisingly, nearly 1 in 5 (19 percent) of these listings contain anti-vaccine keywords or rhetoric in their product descriptions. This suggests that many of the users purchasing these illegal cards are doing so for political reasons. Some of the most commonly occurring keywords are "government", "forced", "control" or "autonomy". It could also be the case that some Dark Web sellers with anti-government or anti-vax beliefs decided to begin selling CVCs because it aligned with their worldview, though it seems more likely the use of anti-vax rhetoric is a marketing tactic to entice a particularly active demographic on Dark Web forums and cash in on a politically divided culture.

Furthermore, these marketplaces are not exclusive to the Dark Web. More than a quarter (28 percent) of Dark Web CVC listings direct buyers to Telegram, Wickr or other encrypted messaging platforms such as WhatsApp. Despite the privacy implications of these encrypted messaging services, platforms such as Telegram have come under fire for a range of other ethical issues. The prevalence of Dark Web vendors instructing prospective buyers to communicate via alternative platforms presents authorities with an additional channel through which to monitor and gather intelligence on those suspected of distributing fraudulent CVCs.

The sale of CVCs on the Dark Web is a growing niche which poses a significant threat to public health efforts at curbing the pandemic; it wouldn't take many fraudulent cards to undermine a nation's COVID-19 measures.

Furthermore, with several vendors claiming to have privileged access or connections to official healthcare databases, organisations must stay vigilant to outsider and insider cyberthreats by applying strict information and supply chain security measures and conducting regular audits for potentially breached information or intellectual property.

Increasing the sophistication of vaccination verification systems, such as introducing digitised CVCs, is insufficient alone to prevent fraudulent versions. That said, devising solutions that are more expensive to counterfeit could disincentivise illicit production by reducing profit margins.

Unlike other Dark Web ventures such as drug trafficking, cybercriminals may view selling CVCs as relatively low-risk in terms of legal consequences. Authorities would do well to dispel this assumption by devoting more time and resources to CVC investigations, setting high penalties for manufacturing, distribution, and use of such products, and highly publicising these efforts as a deterrent ●

**Dr Gareth Owenson**, CTO and co-founder, Searchlight Security is an internationally recognised and published Dark Web scientist. Gareth co-founded Searchlight Security and now oversees the research and development, software engineering and niche cyber capabilities.