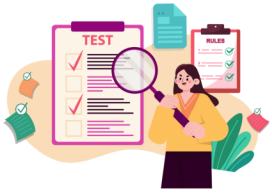


VARDAR ŞANLI FRAUD TEST
MYTH OR FACT

Q1: Gift cards are formal, trackable payment instruments and are therefore considered a safe option even when making payments to individuals you do not know in urgent situations.

○ Fact ○ Myth

Q2: Internal misconduct and fraud cases are believed to be most effectively uncovered during independent external audits, with such audit processes perceived as the primary safeguard mechanism for detecting financial irregularities.

○ Fact ○ Myth

Q3: Emails that contain no spelling errors, appear visually polished, and follow a corporate format are often assumed to be legitimate; professionally crafted and flawless messages are perceived to have a very low likelihood of being phishing attempts.

○ Fact ○ Myth

Q4: Real-time payment infrastructures, by virtue of their transparency and speed advantages, are assumed to inherently reduce fraud risk and significantly limit the potential for misuse.

○ Fact ○ Myth

Q5: Fraud and misconduct incidents are predominantly attributed to external actors, and internal teams are generally regarded as structurally more reliable and as posing a lower level of financial misconduct risk.

○ Fact ○ Myth

Q6: Low-value financial transactions inherently carry limited risk, and it is not possible for small-amount movements to constitute a strategic threat to the institution.

○ Fact ○ Myth

Q7: Fraud attempts predominantly arise as rapidly developing schemes executed in a hurried manner, necessitating immediate responsive action.

○ Fact ○ Myth

Q8: As of 2025, internal reporting mechanisms (particularly anonymous whistleblowing hotlines and employee-driven tip-off channels) continue to constitute the most effective tools for detecting fraud.

○ Fact ○ Myth

Q9: A substantial portion of contemporary financial crime cases is no longer carried out through a single method but through multi-layered and coordinated structures in which several complementary attack vectors are orchestrated either simultaneously or sequentially.

○ Fact ○ Myth

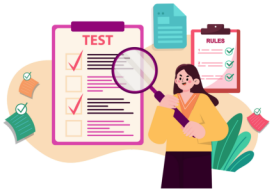
Q10: Illicit proceeds are predominantly laundered through traditional banking channels, and therefore the highest concentration of money-laundering risk within the financial system is still perceived to lie in conventional bank accounts.

○ Fact ○ Myth

FRAUDWEEK.COM
FRAUD AWARENESS WEEK
2025 OFFICIAL SUPPORTER

VARDAR | ŞANLI

INTERNATIONAL FRAUD AWARENESS WEEK
November 16–22, 2025



VARDAR ŞANLI FRAUD TEST
MYTH OR FACT

A1: MYTH Gift cards, due to their significantly limited traceability and reversibility compared to traditional banking products, are among the payment instruments most frequently exploited by fraudsters.

A2: MYTH The ACFE Occupational Fraud 2024 report demonstrates that independent external audit processes are far less effective in detecting fraud than commonly assumed; when compared with employee tips, anonymous hotline mechanisms, and continuous internal monitoring systems, their detection rates remain markedly lower.

A3: MYTH Contemporary phishing attempts are engineered with such sophistication, leveraging advanced social engineering techniques and AI-powered content-generation tools, that they are often virtually indistinguishable from genuine corporate communications.

A4: MYTH Real-time payment infrastructures, by settling transactions within milliseconds, enable fraudsters to rapidly disperse illicit funds or transfer them through successive accounts; this significantly weakens both the detection window and the prospects of recovery.

A5: MYTH Data from 2025 clearly indicates that a significant portion of high-value and institutionally damaging misconduct cases originate not from external actors but from internal sources or individuals directly linked to the organisation.

A6: MYTH The widespread assumption that low-value financial movements carry only limited risk has lost its validity within the modern payments ecosystem. Today, schemes classified as “micro-fraud” and “micro-laundering” clearly demonstrate that individually insignificant transactions, when repeated at high frequency, can cumulatively result in losses amounting to millions.

A7: MYTH In particular, low-profile misconduct patterns characterized as “slow-burn fraud”, which unfold over months or even years, have become major contributors to overall corporate losses. Gradually increasing expense items, incremental supplier price manipulations, systematic data deletion, and the persistence of minor irregularities collectively form structures that account for a substantial portion of total harm. Accordingly, fraud does not manifest solely through fast-moving attacks but also through slow-advancing, low-visibility schemes whose cumulative impact is considerably greater.

A8: FACT Despite advancements in behavioral analytics and automation, ACFE’s latest reports indicate that the majority of detected cases still come to light through employee reporting.

A9: FACT In the contemporary fraud landscape, conducting attacks through a single channel has become the exception rather than the norm; instead, a “multi-vector social engineering” approach, integrating multiple communication and verification layers such as email, deepfake voice technologies, social media interactions, and fraudulent payment interfaces into a single attack sequence, has emerged as the predominant method.

A10: MYTH Findings from the 2024–2025 period indicate that the primary conduit for laundering illicit proceeds is no longer traditional bank accounts; instead, complex transaction networks built through fintech-based infrastructures, digital wallet ecosystems, online gaming platforms, and international payment service providers have become the dominant channels.

FRAUDWEEK.COM FRAUD AWARENESS WEEK 2025 OFFICIAL SUPPORTER

VARDAR | ŞANLI

INTERNATIONAL FRAUD AWARENESS WEEK
November 16–22, 2025