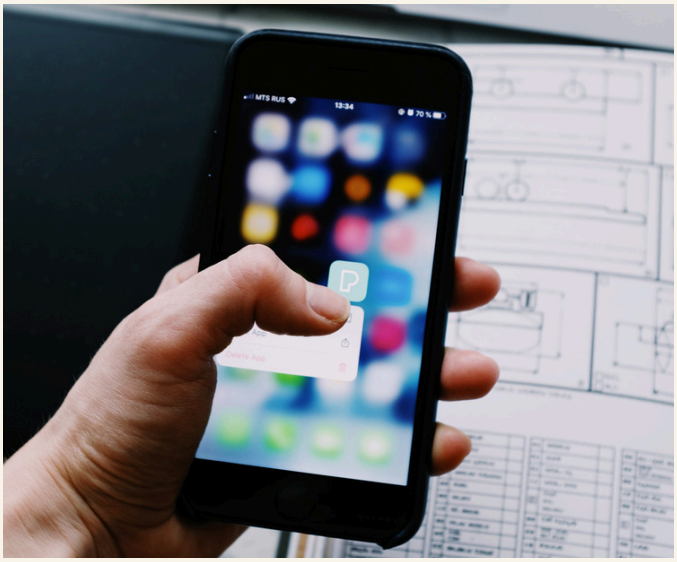
CYBER TRAP:

FRAUD THROUGH APPLICATION PROGRAMMING INTERFACE ABUSE

HOW DOES API ABUSE BECOME A TRAP?



An Application Programming Interface ("API") can be described as a set of rules, protocols, and tools that enable different software systems to communicate and exchange data with each other. As a cornerstone of digital infrastructure, when the security of these interfaces is neglected, unauthorized use of APIs can lead to data theft, account takeovers, and illicit financial gain.

Common exploitation methods involve sending an excessive number of requests in a short time to overload system capacity, exploiting vulnerabilities to gain unauthorized access to customer data and financial information, abusing promotional campaigns or discounts, creating multiple accounts using fake or stolen data, and manipulating API parameters to bypass transfer limits or exploit discounts.

New-generation fintech applications, e-commerce platforms, and digital membership systems are among the sectors most at risk from these attacks.

LEGAL ASSESSMENT:

- ***TCC Article 243:*** Unauthorized access to systems via an API may constitute the offense of "*unauthorized access to an information system.*"
- ***TCC Article 244:*** Using API exploitation to disable a system or alter data may constitute "*hindering, disrupting, destroying, or altering a system or data.*"
- ***TCC Article 136:*** Accessing personal data through API vulnerabilities may constitute "*illegally providing or obtaining data.*"
- ***TCC Article 158/1-f:*** Gaining unjust benefit through promotions, transaction manipulation, or similar API exploitation may constitute "*aggravated fraud committed by using information systems.*"
- ***TCC Article 282:*** Channeling proceeds obtained via API abuse into financial systems may constitute "*laundering of criminal assets.*"

CYBER TRAP:

FRAUD THROUGH APPLICATION PROGRAMMING INTERFACE ABUSE

WHICH PRECAUTIONS SHOULD BE TAKEN?

- Set request limits for APIs to block abnormal traffic *(rate limiting)*.
- Implement strong authentication mechanisms and regularly review access rights.
- Encrypt sensitive data both in transit and at rest.
- Install real-time API traffic monitoring and alert systems to detect suspicious patterns.
- Provide regular training to technical teams and other staff on API security and cyber fraud methods.

VARDAR ŞANLI IN ACTION:

- We provide corporate legal advisory services and conduct risk assessments in line with relevant national and/or international regulations, particularly on anti–money laundering, personal data protection, and MASAK obligations, while also delivering in-house training programs.
- We design API usage policies, license agreements, confidentiality provisions, and corporate procedures relating to API access, data sharing, and third-party integrations to minimize fraud risks.
- We manage criminal and civil proceedings involving this type of fraud with a comprehensive and confidentiality-focused approach and, through our international partnerships, deliver swift and effective cross-border solutions.