ID THREAT COMPETITIVE ANALYSIS - GOVERNMENT ID VS PAYMENT/EMV CARDS VS DYNAMIC PARTIAL ID

TYPE ID		GOVERNMENT ID		PAYMENT CARD		DYNAMIC PARTIAL ID	
FORM FACTOR		PHYSICAL	VIRTUAL	PHYSICAL	VIRTUAL	PHYSICAL	VIRTUAL
THREAT	DESCRIPTION	THREAT MITIGATION					
Card Skimming	A fraudster gets victims' ID details via skimming devices (NCF/RFID), hidden cameras etc. followed by data extraction. This data is misused later.	NO	YES	NO	YES	YES	YES
Man-in-the-Middle	The attacker intercepts the card details while they are in transit (e.g. weak Wi-Fi). In this case, the attacker appears as the relying party to the user and as the user to the target server.	NO	NO	NO	<NO>	YES	YES
Phishing, Vishing, Smishing	The attacker targets unsophisticated and unsuspecting victims and fools them into sharing their card details. The attack is launched via email, website, phone calls or SMS.	NO	NO	NO	<NO>	YES	YES
Pharming	The attacker poisons the DNS server & redirects users to the fraudulent web site. Users do not suspect anything wrong because the user selects the genuine web site from a saved favourite or actually types in the correct URL.	NO	NO	NO	<NO>	YES	YES
Fraudulent Admin or DB Breach	A fraudulent administrator gets access to PII on the backend server and misuses it. It is true in case of a database breach as well.	NO	<NO>	NO	<NO>	YES	YES
Replay attack	This attack follows from card skimming, MITM, phishing, pharming, inside fraud or DB breach. Compromised (harvested) data is misused (replayed) at a later time to perpetrate identity theft.	NO	YES	NO	<NO>	YES	YES
Key Logger	This malware allows the attacker to record all keystrokes and mouse clicks & regularly transmits the credential information to the criminal via the internet.	NO	NO	NO	NO	YES	YES
Malware browser memory attack	Malware attack targets the credentials downloaded in the memory of a system.	YES	YES	YES	YES	YES	YES
Brute Force	Attacker exhaustively attempts all possible combination of missing identity data.	YES	YES	YES	YES	YES	YES
Social Engineering – Shoulder Surfing	While the ID card is being used, a fraudster tries to peek over the victims' shoulder to acquire card details. An advanced form could be spying by covert cameras.	NO	YES	NO	YES	YES	YES
Zero-day Vulnerability	Mobile OS security flaw, for example Pegasus, that is unknown to the OS vendor.	YES	NO	YES	NO	YES	NO
Photocopy Fraud	When a victim needs to avail a specific service, at time of hotel checking etc. they give a photocopy of their identity card. A dishonest employee could mis use the identity ?	NO	YES	N/A	N/A	YES	YES
SIM Swap Attack	A SIM swap attack occurs when Id is linked to SIM & fraudsters convince a telecom provider to transfer a victim's mobile number to a new SIM card that the attacker controls.	<NO>	<NO>	<YES>	<YES>	YES	YES
MFA Vulnerability	Does the ID card/system itself enhance online access 2FA?	NO	NO	NO	NO	YES	YES
User training/ Awareness Campaign	Does the ID system by itself secure identity data or it there dependence on user training or awareness?	YES	NO	YES	NO	YES	YES
Dependence on smart phone/device	Does the technology by itself self-sufficient to secure identity data? Or there is dependence on smart phone or end user computing device?	YES	NO	YES	NO	YES	NO
Broad-Spectrum	Is there effective coverage across entire public and private sector relying parties? Or is there reliance on legislation to offer robust protection?	NO	NO	YES	YES	YES	YES
TOTAL SCORE		5/17	6/17	7/16	6/16	17/17	15/17
PERCENTAGE		30%	35%	44%	38%	100%	88%

LEGEND	YES - 1 Point	NO - 0 POINT	N/A	<RESPONSE>	DATE UPDATED
DESCRIPTION	STRENGTH	LIMITATION/VULNERABILITY	NOT APPLICABLE	SCORING MAY CHANGE WITH DIFFERENT TECHNIQUES	19th JULY 2025