Research Areas

1) Account Takeover (ATO) and Credential Stuffing

What we track

- Credential reuse + automated login attempts ("credential stuffing")
- Unusual login patterns: device changes, IP/location anomalies, velocity spikes
- Post-login behavior: payee/beneficiary changes, refund destination changes, new bank accounts, profile edits

Why it matters

ATO commonly starts with **stolen credentials** and scales quickly through automation. Verizon's DBIR research highlights credential abuse and credential stuffing as a persistent driver of compromise and downstream account misuse.

Controls and signals (high level)

- Step-up authentication for high-risk sessions (risk-based)
- Velocity limits, bot detection, and anomalous session scoring
- Strong authentication guidance aligns with NIST digital identity recommendations (e.g., phishing-resistant MFA approaches).

2) Identity Theft and Synthetic Identity Signals

What we track

- New-account risk indicators: identity inconsistency, rapid attribute changes, thin-file patterns
- First-party vs third-party fraud indicators in disputes and claims
- Multi-account linkages: shared devices, emails, phone numbers, addresses

Why it matters

Industry threat landscape reporting continues to emphasize identity abuse and stolen credentials as major sources of concern across breaches and fraud activity.

3) Fraud Trend Monitoring and "What's Changing"

Trend themes to monitor

- Credential theft + phishing leading to ATO pressure

- MFA fatigue / push-bombing and social engineering
- Faster fraud cycles: short time-to-monetization after compromise

Why it matters
Verizon DBIR research and related analysis continue to point to credential-based attacks and human-factor exploitation (phishing/social engineering) as recurring patterns.

How we present trends

- Weekly/monthly trend notes: top attack paths, top merchant categories impacted, top customer journey points exploited
- KPIs: confirmed fraud rate, false positive rate, loss rate, investigation throughput, time-to-containment

4) High-Dollar Payment Risk and Business Email Compromise (BEC) Awareness

What we track

- High-dollar anomalies and behavioral red flags (especially around payee changes)
- Vendor/payment instruction changes and unusual urgency patterns
- Escalation paths for investigation and reporting consideration

Why it matters
The FBI IC3 annual reporting highlights the scale of internet-enabled fraud losses and tracks major complaint categories, including those tied to payment fraud and compromise patterns.