Most Common Types of Identity Theft and Fraud

In today's data-driven world, companies are generating and managing unprecedented volumes of information. This surge in data—especially customer data—brings significant security challenges, with identity theft being one of the most critical threats businesses face.

Identity theft is a pervasive issue that can impact anyone, from government agencies disbursing social benefits to global financial institutions. What makes it especially dangerous is its unpredictability; you may not know whether you're dealing with the root cause or just the fallout.

In this article, we delve into the fundamentals of identity theft: what it is, how it happens, the signs to watch for, and how businesses can prevent it.

Photo by GuerrillaBuzz on Unsplash

What Is Identity Theft?

Identity theft involves the unauthorized use of someone’s personal or financial information, such as their name, address, Social Security Number, or credit card details, usually for monetary gain. Essentially, the perpetrator impersonates someone else to deceive organizations and gain access to benefits or services.

According to the USAGov website, identity thieves use various techniques to acquire sensitive data, including:

- Stealing wallets or purses
- Dumpster diving for documents like bank statements
- Using card skimmers at ATMs or retail terminals
- Hacking public Wi-Fi networks to extract mobile data
- Phishing via emails, text messages, or phone calls
- Scanning social media profiles for personal details
- Disguising data collection in online quizzes or surveys

Major data breaches also serve as a goldmine for identity thieves.

In some cases, identity theft is even collaborative, where a legitimate account holder shares credentials with unlicensed associates, like in ride-hailing services, creating risks for both customers and businesses.

Identity Theft vs. Identity Fraud

Though often used interchangeably, identity theft and identity fraud are distinct:

- Identity theft is the act of illegally acquiring someone’s identity data.

- Identity fraud occurs when stolen data is used to commit deception, such as creating fake documents or misusing legally obtained information.

In other words, identity theft is usually the precursor to identity fraud. However, identity fraud can also occur without theft, when legitimate data is misused. Both result in financial losses and reputational harm, with small and large businesses alike being common targets—95% of enterprises and 90% of SMBs experienced identity fraud in the past year.

Common Types of Identity Theft

Identity theft can take many forms. Some of the most prevalent include:

1. Child Identity Theft

Criminals exploit children’s data, like Social Security Numbers, to open bank accounts, apply for government benefits, or rent property. Often, the fraud isn’t detected until the child grows up and applies for credit or loans, making prevention and parental vigilance essential.

2. Criminal Identity Theft

Offenders use someone else’s information to avoid legal consequences. For instance, a thief might present another person’s driver’s license when stopped by police to conceal their own criminal record.

3. Financial Identity Theft

The most widespread form, where personal information is used for financial gain, such as unauthorized online purchases, opening credit lines, or committing insurance fraud.

4. Medical Identity Theft

This occurs when someone impersonates another individual to receive healthcare services. Victims may discover unfamiliar procedures or debts in their medical history. Healthcare data breaches are a primary source of stolen medical identities.

5. Synthetic Identity Theft

In this sophisticated scheme known as synthetic identity theft, fraudsters blend real and fictitious information—e.g., a real SSN combined with a fake name—to create a new, “synthetic” identity. These identities are often used to build credit and secure loans before disappearing with the money.

Industry Impact: Who’s Most at Risk?

Sectors most affected by identity theft include:

- Banking and Fintech: Given their financial nature, they remain prime targets.

- Non-banking Financial Institutions: These may lack the rigorous oversight that banks have, making them more vulnerable.

- E-commerce & Payment Providers: Online platforms are increasingly targeted for payment fraud, especially in the EU, where cases are rising year over year.

Fraudsters are no longer isolated amateurs—they're organized, tech-savvy, and increasingly leveraging AI and deepfakes, as noted by the Euro Retail Payments Board.

How to Respond to Identity Theft

Consumers should regularly check their credit reports (via TransUnion, Equifax, or Experian in the US) and set up fraud alerts for early detection. In the event of identity theft, individuals and businesses should promptly report it to the appropriate national platforms in the US, UK, or EU.

Preventing Identity Theft: What Businesses Can Do

1. Follow Regulatory Standards

Comply with industry regulations such as:

- GDPR (EU)

- Red Flag Rule (US)

- AML/CTF laws

- KYC guidelines
- PCI DSS
- eIDAS and ESIGN Acts

These frameworks emphasize robust identity verification procedures and data protection measures.

2. Educate Customers

Awareness is a strong defense. Inform your customers about common scams, especially during high-risk seasons, and empower them to recognize fraud attempts.

3. Train Employees

Regular cybersecurity training and phishing simulations help staff spot red flags and prevent breaches. Training should cover data handling, password hygiene, and social engineering tactics.

4. Implement Multi-Factor Authentication (MFA)

Combining biometrics with one-time codes or passwords ensures higher security. For example, Regula's Face SDK allows real-time biometric verification with minimal friction.

5. Automate Identity Verification

Automated ID checks using biometric and NFC-based tools enable secure onboarding and transaction processing. For instance, top-tier banks now offer account setup within minutes using Regula Document Reader and Face SDK.

6. Regularly Review Security Policies

Threats evolve quickly—your security posture should too. Conduct annual audits and immediate reviews after major organizational changes or incidents.

Final Thoughts

In a world where digital transformation is accelerating, identity theft remains a serious and evolving threat. Cybercriminals are constantly developing more advanced ways to deceive both individuals and organizations.

A proactive, layered approach—combining education, regulation, automation, and modern verification tools—is key to staying one step ahead. Regula provides robust, customer-friendly solutions that help businesses verify identities with confidence.