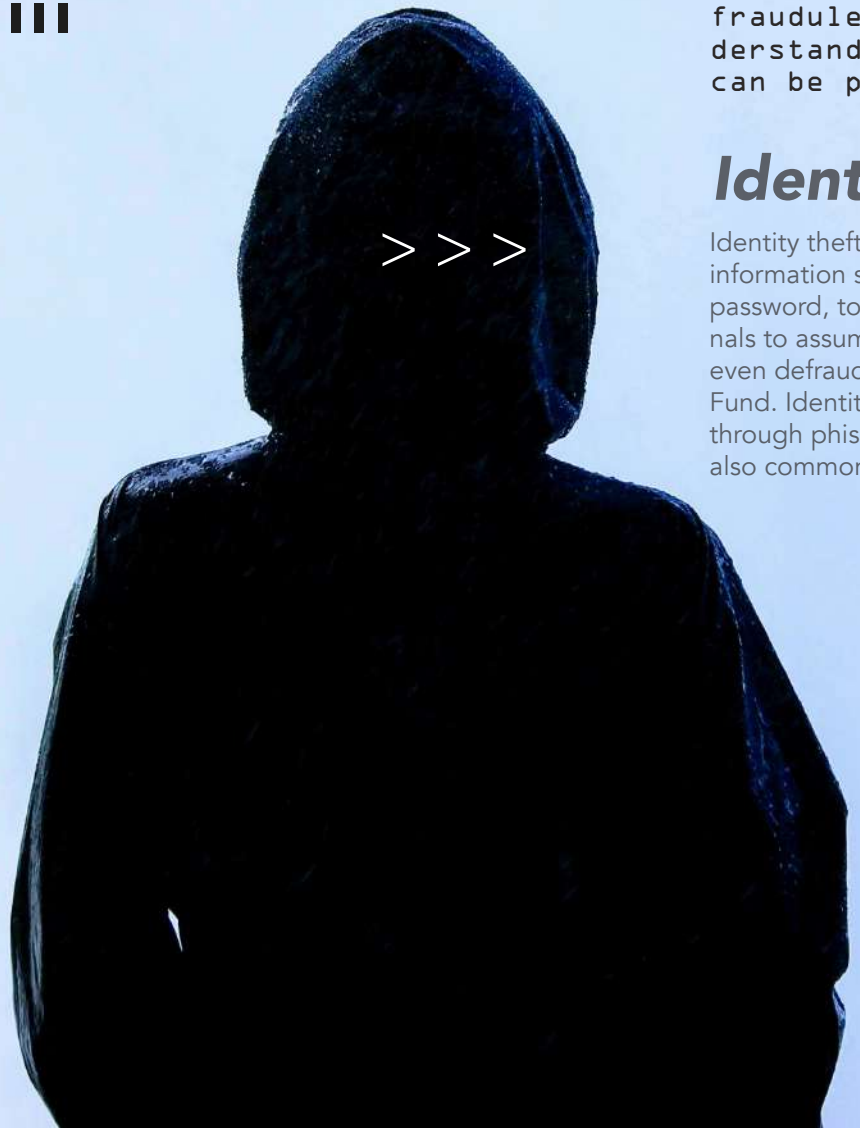
Fraud



In order to defend your business against fraudulent activity, it is important to understand the different types of crimes that can be perpetrated. These can include:

Identity Theft:

Identity theft is defined as someone using personal identifying information such as an ID number, bank account number, username or password, to commit fraud. Personal information can be used by criminals to assume a person's identity and acquire retail or bank accounts, or even defraud insurance, medical aid and the Unemployment Insurance Fund. Identity scammers have various ways of getting details, such as through phishing sites and emails, spoofed websites, and SIM swaps are also common to this type of fraud.

Dynamic Recovery Services

A CYBER 1 Company

Fraud

Bank Fraud

While the specific elements of banking fraud laws vary depending on jurisdictions, it is aimed at defrauding a financial institution as well as the customers of the financial institution.

- Unauthorised trading to recoup the loss incurred in earlier trades
- Fraudulent loans: The "borrower" declares bankruptcy, vanishes or is a non-existent entity
- Fraudulent loan applications varying from individuals using false information to hiding their credit history
- Corporations using accounting fraud to overstate profits

- Wire transfer fraud is also considered bank fraud
- Bill discounting fraud
- Payment card fraud, including non-card present transactions such as online purchases and internet banking transactions

- Phishing, also known as internet fraud

A CYBER 1 Company

Fraud

<<< Theft of Classified Information:

If sensitive information that requires protection of confidentiality, integrity, or availability is stolen, cybercriminals can use the information to commit other types of fraud or sell it to other criminals. Access to classified information is restricted by law or regulation to particular groups of people, and mishandling can incur criminal penalties and loss of respect. A formal security clearance is often required to handle classified documents or access classified data.
The clearance process usually requires a satisfactory background investigation. Like government organisations, some corporations also assign sensitive information to multiple levels of protection, either from a desire to protect trade secrets, or because of laws and regulations governing various matters such as personal privacy, sealed legal proceedings and the timing of financial information releases.
This type of fraud can lead to reputational damage or fines being imposed by a governing body or legislation. It can also lead to financial losses as this information can then be used for identity theft as well as bank fraud.

We run tests and carry out audits that help protect data and prevent fraud. We have a wide range of services that also includes staff training on fraud and security risks, as well as multi-factor authentication, data loss prevention, and remediation. We help customers develop the organisational understanding to manage fraud risk, and then to develop and implement the appropriate safeguards. We help identify fraud and take the appropriate actions to restore any capabilities or services that were impaired as a result of it. Our skill set and experience enable them to assist in building and maintaining a secure network, protecting data and implementing strong access control measures. We help maintain a vulnerability management programme, as well as the vital security policies necessary to help stop fraud in its tracks.