CASE STUDY: CYBERCRIME

The FIC was part of a multi-agency investigation after cyber-attackers gained access to the bank accounts of two financial institutions and transferred large sums of money to several beneficiary accounts. The FIC traced and identified these multiple bank accounts, and tracked the flow of funds to block the accounts.

In the first attack, R72.2 million was illegally transferred into 1 433 different accounts, and was immediately dissipated. These beneficiary accounts – mainly dormant accounts – were accessed with legitimate login credentials stolen by loggers and/or spyware. A complicit bank employee created duplicate cards to access these accounts.

In the second incident, a syndicate, with inside help, hacked into a bank's computer systems and transferred R42 million to a large number of beneficiary accounts. These amounts were immediately withdrawn using ATM cards with increased daily limits. Analysis determined that two of the financial institution's PC workstations had been cloned to enable the fraudulent transfers.

The FIC created profiles on the beneficiaries of these transactions and identified various suspects and related bank accounts and investment portfolios. Cell phone data supplied by investigating authorities was analysed and links between suspects were identified. As a result of the joint operation, several suspects were arrested. Information supplied by the FIC was used to support preservation orders on immovable and movable property, such as expensive houses and vehicles.