CASE STUDY

Fraudulent Activity via Internet Banking

Q4 2023

Introduction

The Financial Intelligence Agency (FIA) is Bermuda's Financial Intelligence Unit (FIU), established in part to meet the recommendations of the Financial Action Task Force (FATF), including FATF Recommendation 29, which calls for countries to establish an FIU that serves as a national centre for the receipt and analysis of suspicious transaction reports and other information relevant to money laundering, associated predicate offences, and terrorist financing, and for the dissemination of the results of that analysis.

In carrying out its functions, the FIA collects Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs) from regulated entities and others, as required under Bermuda's Proceeds of Crime Act (POCA). The FIA then analyses the data provided to uncover activities and patterns that may indicate money laundering, terrorism financing, or other related criminal activities. This intelligence is disseminated to local law enforcement, regulators, and certain international partners.

About Case Studies

Case studies published by the FIA are sanitised, representative examples of intelligence cases disclosed by the FIA during the reporting period. As part of the FIA's commitment to the fight against money laundering, terrorist financing, and related crimes, case studies are produced to assist reporting entities in identifying and reporting suspicious activity.

Indicators and Red Flags

The FIA has identified indicators of money laundering and terrorist financing within its case studies. These indicators are generalised underlying principles identified by the FIA and its international partners. A list of common identifiers has been compiled and coded into the FIA database. When filing a SAR, reporting entities are able to choose from a list of over 100 indicators. In the context of individual case studies, an indicator can be considered a "Red Flag" which could serve as a basis for suspicion by a reporting entity.

Case Study: Adverse Media involving Life Insurance Policy Surrender

SAR Details

The FIA received a SAR filed by a local bank. A long-time client was contacted by an individual claiming to represent a trusted local telecommunications provider. The client's internet banking was compromised, and a wire transfer of USD $270.00 was sent to an overseas bank account. The client was locked out of her internet banking platform. The bank identified two additional reports in the preceding 15 months involving the same tactic: an individual claiming to represent a telecommunications provider. In one case, the victim suffered losses totalling USD $125,643.87 sent to nine different beneficiaries; in another, BMD $7,200.00 was transferred to an account in an overseas financial centre.

FIA Analysis

Analysis revealed classic fraudulent tactics including using a common alias, gaining the victim's confidence by impersonating a reputable provider, obtaining remote computer access, wiring funds overseas to complicate tracing, and locking the victim out of their banking platform. One of the victims had a history of being targeted by fraudsters, with eight previous transaction monitoring investigations. The FIA recommended reporting the fraudulent activity to social services. A spontaneous disclosure was sent to the Customs Department Joint Intelligence Unit.

Red Flags

- Impersonation of a representative from a trusted telecommunications provider.
- Use of a common alias to make tracing difficult.
- Voice phishing (vishing) used to obtain remote access to victims' computers and banking.
- Account takeover resulting in unauthorised transactions.
- Victims instructed to download unfamiliar applications granting full access.