Consumer Education

Subscription Fraud

CONSUMER EDUCATION

Communications Fraud Control Association

Version 1.0

Communications Fraud Control Association

Subscription Fraud

Providing insights, knowledge and learning when it comes to fraud.

DEFINITION:

Subscription Fraud: aka Application Fraud occurs when a new application is submitted with fraudulent details/PII (Personally Identifiable Information) by means of being stolen, synthetic or falsified, with the intent to obtain services that the party doesn't intend to pay for.

Includes the below types:

Synthetic ID Fraud – Creation of a fake identity to obtain service, credit, and other goods/products. Typically, Synthetic ID Fraud scenarios include the following: Manipulated PII, using parts of other people's PII, or created by Auth User Abuse (i.e., credit piggybacking)

PII Manipulation –Person/s manipulating PII to get a subscription that normally defaults for non-pay, or in order bypass past bad debt, or to gain better offers.

Identity Theft - when the full identity (PII) of an existing person is stolen and used fraudulently to gain services or for financial gain

MOTIVATION:

In short, the most prevalent reason for motivation is to gain services, equipment, and financial gain. Motivations also vary by Subscription type, such as Synthetic IDs are created with the purpose to defraud multiple businesses using the same identity (PII). Many Synthetic Identities look and act real, and lay hidden as a subscriber for months (while paying for services), even longer at times, and then 'bust out' after large purchases, and become non-pay. Collections are unable to collect due to identities not being real.

PII Manipulation is also motivated by a consumer or dealer or fraudster to avoid past bad debt with a business, or with intent of non-pay, or bad credit situation where a consumer is gaming the system to see what PII would pass existing controls and provide best offers.

ADVICE TO CONSUMERS:
N/A

SOLUTIONS:
Ensure businesses are using automated real-time frictionless identity verification solutions in the NAO (new application organization) process, layered with specific use case scenarios like Synthetic ID solutions which are often undetected by normal ID Verification solutions, and supplemented by adding some friction using authentication tools on risky consumers or transactions. Solutions vary with focus on data (PII, digital data, behavior analytics) and device fingerprinting using predictive analytics, machine learning, proprietary data, known fraud data, and 3rd party data to score or flag suspect applications. Best practices cover multiple use cases and ensure businesses are red flag compliant.

Communications fraud is the use of telecommunications products or services with no intention of payment. Fraud negatively impacts everyone, including residential and commercial customers. The losses increase the communications carriers' operating costs. Although communications operators have increased measures to minimize fraud and reduce their losses, criminals continue to abuse communications networks and services. Therefore, communications operators tend to keep their actual loss figures and their plans for corrective measures confidential. Due to the sensitive nature of this topic, CFCA used a confidential opinion survey of global communications operators to support the global fraud loss study.

About CFCA

CFCA is a not-for-profit global educational association that is working to combat communications fraud. The mission of the CFCA is to be the premier international association for revenue assurance, loss prevention and fraud control through education and information. By promoting a close association among telecommunications fraud security personnel, CFCA serves as a forum and clearinghouse of information pertaining to the fraudulent use of communications services. For more information, visit CFCA at www.CFCA.org.

Correspondence should be sent to fraud@cfca.org

Disclaimer of Liability

The material and information contained in this document is for general information purposes only. You should not rely upon the material or information in this document as a basis for making any business, legal or any other decisions.

Whilst we endeavor to provide correct information, CFCA makes no representations or warranties of any kind, express or implied about the completeness, accuracy, reliability, suitability or availability with respect to the information and graphics contained in this document for any purpose. Any reliance you place on such material is therefore strictly at your own risk.

CFCA will not be liable for any false, inaccurate, inappropriate or incomplete information presented in this document.

To the extent not prohibited by law, in no circumstances shall CFCA be liable to you or any other third parties for any loss or damage (including, without limitation, damage for loss of business or loss of profits) arising directly or indirectly from your use of information contained in this document.

www.cfca.org

Communications Fraud Control Association