New Account Fraud- A new breed of scams

Overview

Criminals are always probing defences and finding new ways of committing fraud at scale, while also taking precautions to stay undetected. As the lenders extended applications to the digital channels, fraudsters have also followed and piled into the digital world and with years of experience under their belts, they are developing various tactics to diversify their targets.

One of those evolving frauds is new account fraud. And, as the organisations of all kinds become increasingly dependent on customer onboarding using mobile devices, they became avenues for the fraudsters. Dealing with new account fraud risk has become more complex than ever before. With increasing fraud cases and losses burgeoning, many organisations seem to be far from ready.

Outline

Introduction

Banking customers around the world conduct more of their business online more than ever. According to Capgemini, by 2022 global non-cash transactions are expected to reach $1 trillion [1]. But as more customers move online so do cybercriminals.

There are of course multiple frauds but New Account Fraud (NAF) is the most expensive form of identity fraud to both organisations and consumers.

In new account fraud, fraudsters use stolen or synthetic identities to open new bank, credit and loan accounts and borrow as much money only to disappear at the end leaving behind a trail of endless debt in their wake. Moreover, NAF can also be used to launder money.

Unfortunately, this fraud remains as common as ever further increasing. In 2018 alone, **3.2 million customers** were affected by this fraud [2]. There are a number of factors contributing to make NAF an increasingly complex issue, including; the omnipresence of digital applications, the commercialization of customer data and the highly sophisticated techniques that criminals use. The best hope of tackling NAF lies in leveraging highly advanced technologies, keeping up with the cybercriminals and adopting highly sophisticated means of **securing identity.**

NAF attacks have become immensely sophisticated as fraudsters use strategies to impersonate a victim far beyond a single account, and even go as far as creating new highly effective identities from scratch.

Here are two types of identities that hackers usually create.

Complete impersonation: Fraudsters establish and/or take over a broader range of accounts in an increasingly connected and interdependent ecosystem, including mobile phone, utility, and email accounts that ultimately enable them to be more successful in committing subsequent frauds that affect banks, credit unions, issuers, lenders, and others within the financial services space.

Synthetic identities: An overreliance on validating the relationship between core biographical data elements with the major credit bureaus has encouraged fraudsters to create synthetic identities using Social Security numbers that have not been issued or that belong to children. These identities are subsequently bolstered by consumers.

How does New Account Fraud work?

In most instances new account fraud occurs in four stages;

1. Harvesting the raw data

This is the initial stage of fraud where fraudsters steal personally identifiable information (PII) of the consumers in large quantities by targeting big organisations including financial institutions, mobile network operators, tech providers and others that store information in large volume. This information is then put up for sale in dark marketplaces.

2. Distribution of data

At this phase, the collection of identity data is further enhanced by adding information from social media platforms and other sites. This fully collected identity data is then sold to fraudsters via the dark web and other forums.

3. Account Fraud

The stolen information bought by the fraudsters is used to open financial accounts in the name of the victims and in some cases, the identities are moderated with some fake data with the same end goal. After opening up the accounts they built credit scores and then max out loans and disappear without returning leaving banks and card companies liable for huge losses.

4. Cashing Out

Funds are transferred to other accounts, perhaps in other countries where banking checks are less rigorous, or into mule accounts, some of which may also have been opened using fraudulent identities.

A brief history of fraud

New account fraud wasn't always like this. In the early 2000s, the main threat to the banking firms was counterfeit cards and fraud associated with bank cheques [3]. These frauds were considered relatively easy, cheap and quick ways to make money for fraudsters. While the frauds such as NAF and account takeover frauds required some serious skills and information that wasn't easy to come by and needed some research and planning. Getting identity data wasn't easy to obtain, which means that fraudsters had to put serious skills and resources into social engineering banking staff for the details of their customers. Setting up accounts for laundering the money was more difficult as compared to today. In short. NAF wasn't worth the return on investment (ROI) for the fraudsters.

A decade later numerous inter-connected trends have combined to make NAF and account takeover, a more feasible proposition for the fraudsters. As the development of global standard EMV (Europay, Mastercard. Visa) significantly disrupted the business model of traditional card fraud, more fraudsters became motivated to explore new avenues and opportunities for conducting fraudulent activities. Since more companies began to offer digital services, consumers' personally identifiable information (PII) started to proliferate online. This gave rise to a cyber economy powered by anonymous dark web marketplaces that traded in cyber tools and this stolen information online. Some estimates claim that the underground dark web economy is worth as much as $1.5 trillion annually [4]. And, $160 million of this comes from trading in PII. Some of the sources even claim that this figure is higher. Approximately $16 billion of PII was stolen in the US alone in 2017, according to one report[5].

Three main types of banking fraud emerged from this perfect storm of digitalisation.

1. Account Takeover Fraud

This fraud involves the use of stolen login credentials, obtained using phishing/social engineering or bought online using the dark web, to hack user bank accounts and credit cards. This type of fraud was snowballed major thanks to consumers' negligence of sharing similar passwords over multiple accounts. ATO fraud is very difficult to identify as the fraudsters are using legitimate logins as real customers

2. Transaction/Payment Fraud

As the realtime and cross-border became convenient so do fraudsters' chances to make fraudulent purchases. Payment fraud involves using stolen payment credentials to make fraudulent purchases. This fraud has been causing financial institutes increasing problems in detecting and stopping these attempts.

3. New Account Fraud

New Account Fraud (NAF), is one of the difficult scams to identify because fraudsters use legitimate identity data, also called **synthetic identities,** which have never been used before. It involves taking data, from highly sophisticated breaches or using phishing and social engineering to obtain identity data and often combining it with fake data, to open new accounts in victims' names. Fraudsters then max out loans and other overdraft facilities before moving on.

Current Trends in Digital Fraud

Data Breaches

In 2017, data breaches in the US increased by 44.7%.

Fraudulent Activity

In 2016, 15.4 million new accounts were noted to have fraudulent activity.

Fraud Increased

New account fraud increased by 27.8% worldwide YTD in 2019.

NAF

NAF increased by more than 100%

Fraud in Asia-Pacific

The Asia-Pacific region experienced the highest rates of full-year fraud at 3.27%

Gaming / Gambling

The cryptocurrency and online gaming/gambling industries experienced higher-than-average fraud levels.

Biggest banking markets

In the UK, NAF surged by a staggering 159% year-on-year to reach £29.4 million ($38m) in 2018.

[1] Iovation

[2] Helpnet Security

Tactics Used by Fraudsters

New Account Fraud is one of the rapidly increasing types of fraud. With rise almost double to the year 2014, it is creating threat alarms for the online marketplaces [6]. To summarise the rise in new account fraud, here are some of the tactics and trends used by fraudsters:

Data Breaches

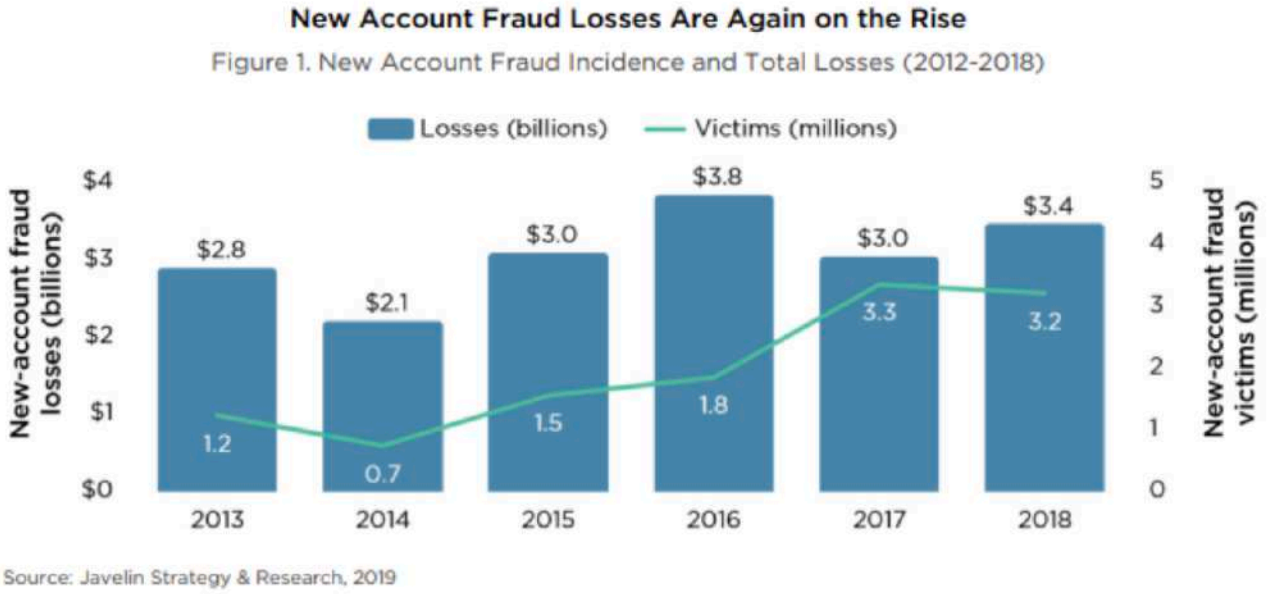
Data breaches and information theft using social engineering are the biggest sources for personal data that fraudsters use to conduct NAF. These data breaches incidents provide a continuous influx of personal data to the dark web where it is bought by identity fraudsters. This data includes everything from passports and driver's licenses to credit card info, social security numbers and government ID, diplomas and account logins.

Synthetic Fraud

Creating an identity by blending real identity with fake identity information has helped in driving new account fraud. In 2013, the DOJ in the US charged 18 people in one of the biggest, most complex credit card fraud schemes ever after a decade-long investigation spanning eight countries [7]. This crime ring developed more than 7000 synthetic identities to fraudulently obtain over 25,00 credit cards. The fraudsters then built up the synthetic identities' credit score to increase their spending and borrowing power, before disappearing without paying. This model of operation is typical to synthetic fraud. This type of fraud alone costs $16 billion in 2016.

Sophisticated Cyber Marketplaces

Cybercrime is a highly organised and sophisticated industry that generates annual revenue estimated to be worth more than the annual GDP of most countries in the world. Dark web and a ready supply of hacking tools are one of the main reasons for the rise in this marketplace. This makes the pipeline of stolen identity data undiminished despite the best efforts of global law enforcement.



Source: Javelin Strategy & Research 2019

Never ending consequences of the New Account Fraud

Given the statistics and evolution provided above it is clear that NAF is on the rise and it shouldn't be surprising at all. Although it's hard to converge global stats, a survey conducted in 2018 highlights that 52% of US financial institutions believe that NAF increased over the past few years [8]. Another study from Javelin reported that losses from NAF in the US increased from 3 billion to $3.4 billion. So it wouldn't be wrong if we call **NAF- a multi-billion dollar problem.**

New Account Fraud has been a staggering problem for some years now and it not only results in financial losses but also has far-ending consequences on the financial institution. Here are some of the potential impacts.

Direct losses from fraud

When fraudsters successfully open new accounts and drain their credit limits, banks face the consequences and remain on the hook for potentially hundreds or thousands of dollars in liabilities per account.

Negative reputation

If a bank accumulates a bad reputation owing to frauds and security it creates a negative impact on the customers and with the advent of PSD2 in Europe [9], it has become difficult to open new accounts with rival financial companies. If multiple customers have a poor experience and they take it to the internet by sharing negative reviews and comments, banks' reputation will be damaged.

Lost Business

If a financial institution decides to place stringent checks that are cumbersome or tiring most of the customers will withdraw during the onboarding process which could result in losses higher than those resulting from fraudsters stealing money.

Time to Act- How FIs can protect against New Account Fraud?

NAF is hard to spot. Fraudsters either use legitimate information stolen secretly from real consumers, or they stitch together synthetic identities using this and fake info. Either way, it can be difficult for traditional filters to detect using threat intelligence feeds and static data.

However, placing **ID documents checks** and physical **biometric checks** could help in correctly identifying the fraudsters.

Using **identity verification** tools like document scanning or digital identity networks alongside risk assessment like KYC and biometrics can meld verification that the identity exists and is legitimate with an assurance that the individual applying is not a fraudster and truly owns the identity being claimed.

Shufti Pro’s approach to identifying and eliminating fraudsters during account opening or customer onboarding could easily help in catching fraudsters while keeping the real customers intact by providing frictionless onboarding.

Shufti Pro uses advanced AI-based technologies to detect and deter fraud. AI-based **document verification** enables quick and secure customer onboarding while accurately detecting any fraud attempt to forge the identity documents. And to further enhance the onboarding process, **facial verification** supported with **3D liveness detection, 3D depth perception, Anti-spoofing checks** and **fake image detection** removes the probability of fraudster getting in unchecked.

All this process takes **15-60 seconds** while delivering accurate results and providing frictionless onboarding to legitimate customers.

Have questions? Contact us and learn how we can help you.

Get your free trial now

🌐 www.shuftipro.com

✉ sales@shuftipro.com

References

1 https://www.bloomberg.com/press-releases/2019-09-17/capgemini-se-world-payments-report-2019-non-cash-payments-booming-as-banks-face-change

2 https://www.javelinstrategy.com/coverage-area/evolution-new-account-fraud

3 https://core.ac.uk/download/pdf/30624246.pdf

4 https://www.information-age.com/global-cybercrime-economy-generates-over-1-5tn-according-to-new-study-123471631/

5 https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

6 https://www.ey.com/Publication/vwLUAssets/ey-global-fraud-survey-2016/$FILE/ey-global-fraud-survey-final.pdf

7 https://www.nj.com/news/2013/02/18_charged_in_200m_credit_card.html

8 https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-study-fraudsters-seek-new-targets-and-victims-bear-brunt

9 https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

10 https://www.idtheftcenter.org/images/page-docs/NewAccountFraud.pdf

11 https://www.acfe.com/uploadedFiles/Shared_Content/Products/Self-Study_CPE/Financial%20Institution%20Fraud%202013_Chapter%20Excerpt.pdf

12 https://www.sas.com/en_us/whitepapers/faces-of-fraud-108403.html

13 https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-study-fraudsters-seek-new-targets-and-victims-bear-brunt

14 https://www.ey.com/Publication/vwLUAssets/Global_Fraud_Survey_2016/$FILE/ey-global-fraud-survey-final-2016.pdf

Shufti Pro True Identity Builds Trust

Expanding services to 230+ countries and territories in a short period of time, Shufti Pro envisioned playing a pivotal role in creating cyberspace where every transaction is verifiable and secure. With enough experience in technologies like machine learning (ML), OCR, artificial intelligence, and Natural Language Processing (NLP), Shufti Pro strives to provide the best identity verification services to verify customers and businesses online.

Shufti Pro's cost-effective solutions help businesses to prevent fraud and illicit crimes that can ruin the integrity and brand reputation of your business. Our perfect solution suite consisting of KYC verification, AML screening, ID verification, Facial Recognition, Biometric Authentication, Video KYC, OCR, and KYB helps to improve your company's fraud prevention, Know your Customer (KYC) and Anti Money Laundering (AML) regulatory efforts by automating the workflow. With single API integration, Shufti Pro empowers you to verify customers with document checks from 3000+ ID templates and business entities from 200 million companies data.

Disclaimer: No warranty or claim is herein provided that information contained in this document is accurate, up-to-date, and/or complete. All information provided in this document is limited for general informational purposes only. In no circumstance(s), does such information constitute as legal or any other advice. Any individual or company who intends to use, rely, pass-on, or re-publish the information contained herein in any way is solely responsible for the same and any likely outcomes. Any individual or company may verify the information and/or obtain expert advice independently if required.