NICE
ACTIMIZE

Insights Article

Reading the Tea Leaves – 2022 FRAML Outlook

2021 has been a dynamic year for fraud and financial crime, and the events that have emerged out of the quickly changing risk landscape continue to create new vulnerabilities for financial services organizations (FSOs).

Key fraud and AML trends of the past year have been particularly prevalent and are positioned to become an even greater threat for FSOs and their customers in 2022. With the new year edging closer, below is a closer exploration into the anticipated trends for 2022 and what FSOs can expect to face as they shape their long-term risk management efforts and technology investment priorities.

4 Pillars that Defined 2021

Faster payments and digital acceleration have played major roles in the evolution of key fraud and AML trends. These conditions are spawning a breeding ground for scams and leading to faster identity theft and a profound spike in data breaches. Fraudsters and cybercriminals are using the instant payments infrastructure and skyrocketing online activity to gain access to sensitive information and take advantage of weaknesses in fraud prevention systems and authentication controls and technologies. Consequently, four critical trends have shaped the risk landscape this year.

Account Takeover (ATO)

ATO fraud attacks have been drastically increasing in 2021, with recent research revealing that 64 percent of financial institutions are experiencing higher rates today than before the onset of the pandemic. Generally, ATO stems from identity theft and entails unauthorized access to a legitimate customer's online account to facilitate fraud and financial crimes. ATO is challenging to detect because it can often go unnoticed by a legitimate account owner, whether that's a business or an individual customer, for a significant period of time. Cybercriminals can alter login and contact details to prevent the actual account owner from quickly realizing that they have been compromised.

Mobile Consumer Fraud

Mobile banking and the integration of instant payment channels, such as Venmo and Zelle, have answered growing consumer demands for convenient digital banking services. While mobile banking presents opportunities for FSOs to improve customer engagement and deliver memorable digital-first experiences, it has also opened the gates to more financial crime and fraud and introduced new challenges in fraud management. Organizations are struggling to maintain the momentum of faster payments and secure faster payment channels while optimizing friction during authentication.

Data Breaches

In 2021, data breaches have already exceeded the total amount in 2020 by at least 17 percent, with approximately 281.5 million people impacted. Data that has been compromised from these breaches includes broader sets of personally identifiable information (PII), as well as partial information, like birth dates and addresses. This sensitive data is then used by fraudsters and financial criminals to fuel diverse schemes and attacks, such as committing application fraud via synthetic identities, for example. Data breaches are widely commoditized on the Dark Web, which has resulted in a normalization of compromised PII and by extension, a surge in complex fraud activity.

Dark Web Activity

The Dark Web is a lucrative resource for cybercriminals and serves as an illicit marketplace and open exchange for stolen information at scale. Bad actors can cheaply procure sensitive data, financial mules and synthetic identities, as well as a range of underground services to augment their crimes, in addition to sharing anti-fraud and evasion tools and controls. Also, FSOs of all types, sizes and in all regions are targeted by large criminal networks, who mobilize on the Digital Underground to organize campaigns against these institutions. The quantity of data and activity available throughout the Dark Web has exponentially grown recently, powered by the growth of data breaches, increasingly advanced cybercrime tools, and the massive adoption of digital banking and online activity.

2022 Forecast

The current pace of digital acceleration is persisting alongside the ongoing pandemic as organizations scramble to advance and sustain their digital-first agendas amidst market, social and economic disruption and the rampant acceleration will exacerbate these key trends in 2022.

FSOs must effectively prepare for waves of attacks against their organization, assets and customers, which is likely to manifest in the form of highly sophisticated, diverse and automated fraud and financial crime threats. Exposure to new and emerging fraud vectors and complex fraud risks, developing terrorism financing and money laundering risks, and threat types that are sliding across all channels and products will culminate in an exacerbated threat environment exceeding anything previously experienced.

Cybercriminals will be exploiting and weaponizing the data that was purchased on the dark web over the course of the past year; there's typically an incubation period involved where it can take upwards of a year from the time of purchase to actually using the illegally obtained information, tools or techniques.

Furthermore, the always-connected consumer landscape will contribute to the growth of consumer scams. This issue will only be aggravated by the technological proficiency of cybercriminals who consistently refine their techniques and approaches alongside emerging tools and technologies, the evolving payments environment, changing consumer behaviors, and industry disruption. Advocacy groups continue to insist that FSOs should be liable, and individual consumers are even resorting to threatening banks on social media when fraud occurs. Under these surmounting pressures and as the onus of liability gradually shifts, banks are increasingly stepping up to reimburse consumers in these circumstances.

2022 will be a remarkable year for FSOs, presenting new obstacles in the modernization of fraud prevention and AML programs and digital transformation initiatives. The risk landscape will only grow more complicated, automated and diversified, and organizations must remain vigilant to guard against and stay ahead of the anticipated threats as the new year unfolds.

Don't let 2022 catch you by surprise. With NICE Actimize, you can prepare your organization for any FRAML challenges – known and unknown – you may face in the new year.

Request Demo

1 Fooshee, T. (2020). Key Trends Driving Fraud Transformation in 2021 and Beyond. Aite Group.

2 Chris Morris. The Number of Data Breaches in 2021 Has Already Surpassed Last Year's Total. October 6, 2021. Fortune. https://fortune.com/2021/10/06/data-breach-2021-2020-total-hacks/

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance.

The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

www.niceactimize.com