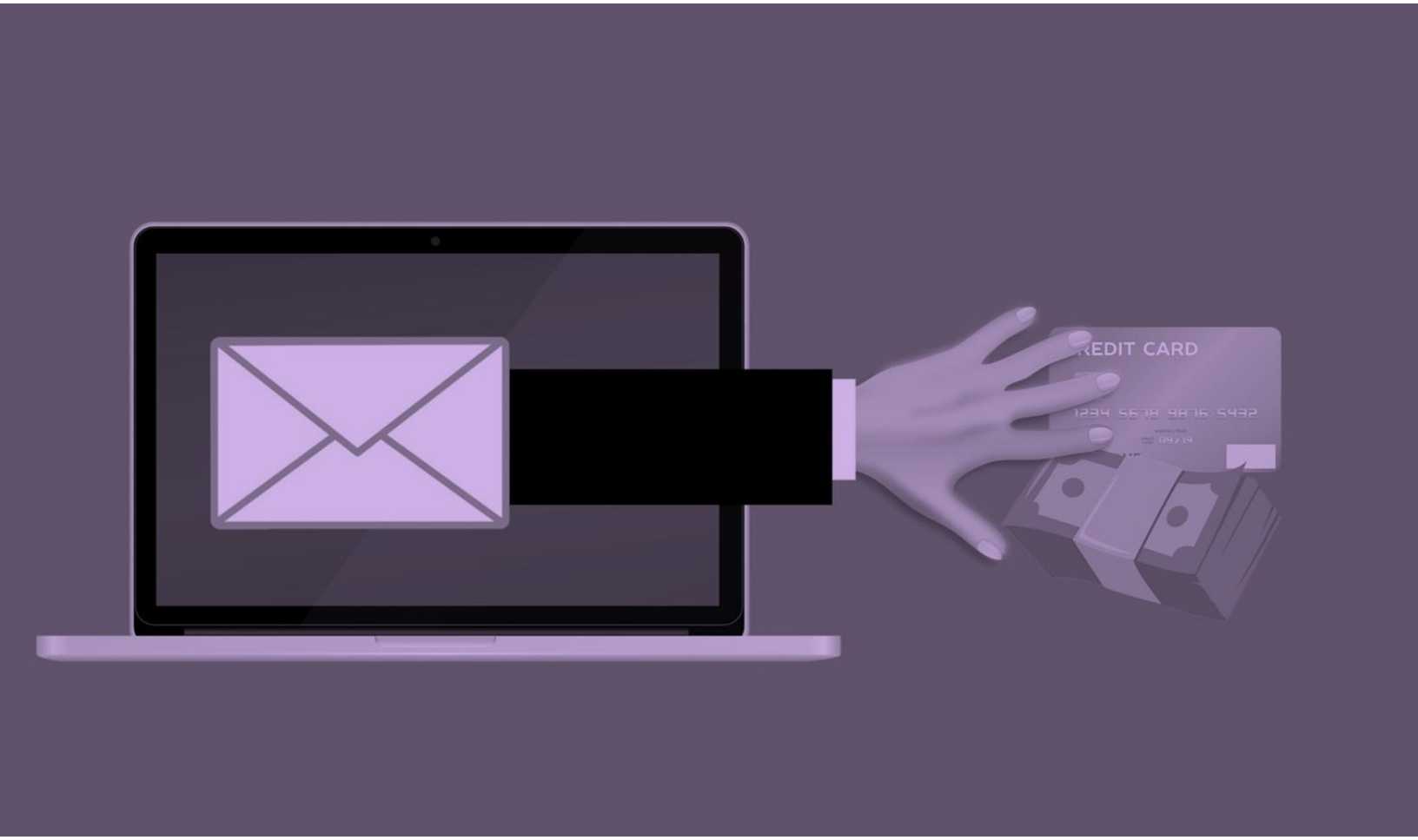
BlokSec

Stop Fraud.
Increase Revenue.



Contents

Summary

The era of digital transformation is accelerating the adoption of online services i.e. eCommerce, banking, and payments. Juniper Research forecasts that nearly half the world will be using digital wallets by 2024, with transaction values to increase by almost 60% to over $9 trillion in 2024.

With the deployment of new and innovative digital services, organizations are able to provide their customers around the clock convenience to access these services. These digital services have also created a medium and an opportunity for the cybercriminals to attack these services via various methods leading to digital fraud – data theft, payment fraud, and account takeovers.

Recent advances in decentralized technologies along with large scale adoption of mobile devices, enables organizations to support widespread deployment of consent-based authorization for their customers. With BlokSec's consent-based authorization, organizations can enable stronger security control that circumvents attacks by cybercriminals.

43% increase in account takeover attack

Source: Nudata

According to Nudata there is a 43% incease in account takeover in 2020 compared to the same period in 2019. These attacks lead to data theft, financial losses, and affects an organization's reputation and brand for years. It is estimated that 32% of victims of account takeover never do business with that organization again.

Over $200 billion in losses

Source: Juniper Research

Juniper Research found that businesses in eCommerce, airline ticketing, money transfer and banking services, will cumulatively lose over $200 billion to online payment fraud between 2020 and 2024, driven by the increased sophistication of fraud attempts and the rising number of attack vectors. These fraud attempts can also include the breach of sensitive information and the compromise of IT systems and data, and a serious loss of brand reputation.

Types of fraud

As new innovations and solutions get deployed, the malicious attackers are keeping pace with these solutions and are finding innovative approaches and attack vectors to support their digital fraud motives.

Some of the most common types of fraud are:

- Account Takeover – is a type of identity fraud where cybercriminals attempt to gain access to a user's (typically consumers) account(s) by updating the account information with their information i.e. update account name, email address, physical delivery address, etc.

- Phishing – is the practice of sending seemingly official emails from legitimate businesses to steal sensitive personal information from users which may include personally identifiable information, user account login details and passwords.
- Identity Fraud – is where cybercriminals acquire and use sensitive personal information such as drivers' license, passport number, social insurance / security number. This stolen information can be used by the cybercriminals to commit fraud against the user.
- Botnets – a botnet is a network of machines controlled by a cybercriminal to perpetuate a host of crimes. In the case of eCommerce, the machine could be used with stolen payment and identity information, so the transaction appears to originate from a location that reasonably matches the credit card in use. In this way, these computers appear to be legitimate, which they are not.

Stop Fraud. Increase Revenue.

With the deployment of new and innovative digital services, organizations are able to provide their customers / end users around the clock convenience to access these digital services. Organizations need to provide their customers / end users with simple and secure experiences to reduce fraud and gain trust.

To enable the next generation of modern authorization, BlokSec has built a platform to support consent-based authorization for important transactions and reduce digital fraud. BlokSec's platform provides security and privacy by design, leveraging a patent-pending consent-based approach for authorization. Advanced technologies like biometrics and cryptography ensure the user identity and authenticity.

BlokSec's consent-based authorization solution allows organizations to enable a step-up authentication and authorization model to curb digital fraud leading to identity theft, payment fraud, and card not present fraud. The enablement of consent-based authorization helps organizations to increase revenue by reducing cost related to fraud.

BlokSec's solution provides a mechanism to request context-specific consent before executing a transaction to ensure that users agree and intend to perform a specific action. This consent driven model offers organizations irrefutable proof of identity and authorization, making the transaction undeniable**.**

The mobile device used as part of the consent-based authorization process creates a unique private key that is stored locally on the device and can only be unlocked using a local gesture such as a biometric recognition (fingerprint scan, facial recognition) associated to the user of the mobile device. This modern approach to authorization ensures that the person is who they say they are – i.e. the account owner – rather than an attacker.

The integration with BlokSec platform can be easily enabled leveraging standards based API. With availability of mobile SDKs for IOS and Android operating systems with full support for white-labeling organizations can provide consent-based authorization as part of their existing application or publish a new application with their branding.

BlokSec's unique approach to transaction logging by leveraging a distributed ledger technology that provides tampered-proof auditing to help organizations to support audit and compliance requirements for important transactions.

Consent-based authorization use cases

Retail

Online retail fraud is estimated to surpass more than $12 billion in losses by 2021 based on a recent study published by Signal Sciences. Account takeover, is the main offender constituting 29.8 percent of all eCommerce fraud.

Here's how it works: When a malicious actor finds or steals user credentials, they enter the account, change their settings i.e. email and phone number, and lock out the user. Next, the malicious actor essentially takes over the account and purchases from the site. They can also run automated tests of the same credentials against other sites.

BlokSec's consent-based authorization provides an added layer of security with near real-time notifications to stop the malicious actors act on behalf of the user to purchase an item without their knowledge and consent.

With BlokSec's consent-based authorization organizations reduce fraud losses and increase their revenue by offering a frictionless transaction authorization experience.

Finance

According to Terbium Labs, credentials for financial accounts ranks in the top five most popular resources for sale on dark web marketplaces. Credentials can be purchased starting from $100+ based on the funds available in the bank account.

Phishing is by far the most common type of attack carried by malicious actors because they prey on a person's fear and sense of panic.

With online payment fraud losses to exceed $200 billion over the next five years, BlokSec's consent-based authorization adds a second layer of security – stopping the malicious actors to act on behalf of the user without their knowledge and consent.

With BlokSec's consent-based authorization, finance / banking organizations can reduce fraud losses and increase their revenue by offering a frictionless transaction authorization experience.

Credit Check

According to the Data Breach QuickView report published by RiskBased security, in 2019 there were 7,098 breaches reported, exposing over 15.1 billion records. This number of records exposed is 284% higher compared to 2018.

With exposure of billions of data containing personally identifiable data including sensitive data, it is a gold mine for cybercriminals to take this data and fraudulently conduct numerous crimes. One approach, for example, that cybercriminals often pursue is to use the sensitive information to apply for a credit card or open a loan account which often requires a credit check – which often does not raise any red flags till sometime in the future when the individual whose identity was used get notifications on outstanding payments.

With integration between a credit check system and BlokSec, the above scenario would not have taken place as the individual would get near real-time notification on their mobile device with the context to make appropriate decision i.e. cancel the credit check request.

With BlokSec's consent-based authorization, organizations can help themselves and their customers from being victims of digital fraud and stop monetary losses related to fraud.

Call / Contact Centre

According to Global Banking and Finance, call / contact center fraud increased by 350% between 2013 to 2019. A common problem for call / contact center's is the method in which users are authenticated. Call center agents are still authenticating customers via information such as phone numbers, date of birth, last 4 digits of social insurance / security number, postal / zip code, etc. These sources of data are freely available to malicious actors on the dark web typically posted after a data breach. Some call / contact centers began to authenticate callers by the sound of their voice, but there is also software available that can change the sound of a caller's voice, which severely negates the benefits of voice-based authentication.

With integration between contact / call center systems and BlokSec, agents can initiate a user verification process requiring customer consent. The customer consent generated by BlokSec is tamper-proof that cannot be forged or replayed.

With BlokSec's consent-based authorization, call / contact centers can help themselves and their customers from being victims of digital fraud and stop losses related to fraud.

BlokSec provides decentralized-identity-as-a-service (DIaaS)™ to support next generation security features to stop account takeovers, phishing attacks, online fraud and identify theft.

Let's keep in touch.

inquiries@bloksec.com | bloksec.com | @bloksec