DIGITAL FRAUD TRACKER®

APRIL 2022

PYMNTS.com | DATAVISOR

Read the previous edition

MARCH 2022

Digital Fraud Tracker®

DIGITAL FRAUD

TRACKER®

PYMNTS.com | DATAVISOR

ACKNOWLEDGMENT

The Digital Fraud Tracker Tracker® was produced in collaboration with DataVisor, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the following findings, methodology and data analysis.

TABLE OF CONTENTS

EDITOR'S LETTER

After years of evolution and uncertainty, cryptocurrencies have taken shape as a valid financial tool. Relatively few consumers have engaged with cryptocurrencies, but most are interested in owning and using them. Their reasons vary, from the desire to have cryptocurrencies as an asset to secure loans, to those who want greater privacy, security or more simplicity in their transactions.

The growing interest in cryptocurrencies accompanies a general lack of understanding among many consumers of exactly how they work, however, leaving them open to scams as fraudsters seek to capitalize on that vulnerability. This is all further complicated by the pseudonymous nature of some cryptocurrency protocols, making transactions difficult to track. Any exchange is permanent and irreversible, the amounts involved can be significant and the transactions themselves are made electronically. Cryptocurrency exchanges and providers have taken steps to guard against fraudulent transactions and account takeovers, though some efforts with multifactor authentication (MFA) have been defeated by flaws in the underlying platforms.

As the cryptocurrency space continues to evolve alongside the need for providers to ensure they are employing best practices in fraud prevention and security, consumers will also have to become more educated on how to be careful. There has been some progress in that regard, as well as a demonstration of consumer interest in better understanding cryptocurrency fraud. To reach a point where cryptocurrency is a fully mature and reliable financial tool, consumers and providers will need to work together with regulators to stay ahead of fraud in this constantly evolving space.

THOUGHT LEADERSHIP TEAM

PYMNTS.com

Feature Story

Wirex On The Challenges And Potential Of Cryptocurrency

Consumers have become increasingly aware of and engaged with cryptocurrencies in recent years. Cryptos are no longer just stores of value or means of investment: The FinTech and banking industry is now offering crypto payment solutions. Crypto cards, for example, enable consumers to make purchases using crypto by automatically and instantaneously exchanging crypto to the local currency.

Procedures and protocols are also maturing, though sometimes at the cost of certain features that crypto users are accustomed to. There are even certain cryptocurrencies called stablecoins where the value of a token is pegged to that of an existing fiat currency to give customers peace of mind regarding volatility.

The number of use cases for cryptocurrency is growing at an unprecedented rate, according to Tony Lees, chief product officer at cryptocurrency platform Wirex, which has 4.5 million users around the globe. As the world becomes cashless, cryptocurrencies will play a significant role, Lees said. They permit fast, easy payments, much like cash but with the added convenience and portability of electronic payments.

“There are huge benefits to crypto payments, namely lower fees, faster payments as well as making cross-border payments much easier and cheaper, making them a hugely important alternative to traditional finance,” he said.

The key to wider consumer adoption will be overcoming misconceptions and educating the general public about cryptocurrency use, Lees explained. Crypto debit cards that make the exchange at the point of sale help consumers feel more comfortable by simplifying the process. That technology can also take the burden off of merchants who are already dealing with the growing number of payment options their customers expect. Rather than adding another payment option, they can accept cryptocurrency but receive the local currency.

“A common misconception around cryptocurrency is that it is overly complicated. But that doesn’t need to be the case when it comes to payments, which is why spending cryptocurrency at the point of sale is crucial,” Lees said. “It means that anyone can hold crypto and spend it without having to worry about keeping up with conversion rates or going through the process of manually exchanging crypto themselves.”

KEEPING CRYPTO SECURE

Lees said recent Wirex research indicated that consumers' second biggest concern about cryptocurrencies after volatility is security and safety. He said most of this comes down to continued misconceptions regarding platform reliability. Platforms such as Wirex are licensed and regulated; furthermore, they prioritize setting their own standards for safety, reliability and security in areas not yet regulated. Wirex, for example, attempts to match the compliance tools traditional financial institutions use.

Security measures protect both customers and the general public by ensuring that Wirex's users are who they say they are and are engaged in legitimate transactions. That means a stringent onboarding process and regular reviews of users' conduct. The trade-off is that Wirex users do not have the same anonymity that is often a selling point for cryptocurrency transactions. Lees, however, believes that is an essential step in crypto becoming a mature and widely accepted means of conducting transactions.

"We believe this transparency is a huge factor in helping to bring crypto into the mainstream and reassuring consumers, businesses and regulators that customers are allowed to use our services and are using them for legitimate reasons," Lees explained.

Customers also get more reliability out of their transactions if they are willing to use cryptocurrency as they would other currencies. Wirex has monitoring systems in place to protect against fraudulent transactions and unauthorized access to accounts. Authenticating both the origin and destination, which is not seen in typical crypto transactions, further protects customers while preventing criminal activity on the platform.

LOOKING TOWARD THE FUTURE OF CRYPTO

Mainstream adoption of cryptocurrencies is very likely in the next few years, Lees said. Cryptocurrencies are already in use for cross-border transactions and by some national governments.

"El Salvador become the first country in the world to adopt bitcoin as legal tender, and other countries like Singapore [are] putting together comprehensive regulation and structures to allow cryptocurrencies to operate as part of the national economy," Lees said. "As more multinational companies, from PayPal to eBay, show their support for crypto and help to develop a global network of crypto services, as well as a growing public demand for easy access to crypto, it's highly likely that more countries and businesses will begin to follow suit in order to establish themselves as key crypto players."

Lees conceptualizes a world in which businesses keep parts of their balance sheets in cryptocurrency as a matter of diversification of investments and even paying employees at least in part with crypto. It could also gain traction in business-to-business transactions. In the coming years, what was once a currency for speculative investments will be more widely used as it was intended in the first place.

Q&A

YINGLIAN XIE
CEO
DATAVISOR

How does fraud affect firms offering products and services in the cryptocurrency space? Which specific fraud considerations should FIs look out for when seeking to launch these products and services?

In some respects, preventing fraud in the cryptocurrency space is similar to [preventing it in] other financial and digital services because FinTechs and FIs offer cryptocurrency products through accounts. Therefore, they must prevent account fraud, which comes in two main forms.

First comes the need to prevent account opening fraud, which can be defined as any attack or criminal activity that targets the customer onboarding process with the purpose of creating fraudulent or false accounts. Criminals provide stolen, false or synthetic identities to gain an entry point and pose as businesses' legitimate customers and use bots and other advanced technological means to mass register accounts and exponentialize the size of the damage they inflict.

For example, crypto exchanges offering new user incentives or other promotions to attract new customers might end up wasting valuable resources instead. Fraudsters often use bots and false or stolen identities purchased in batches by the thousands to mass register accounts, get the bonuses and then abandon the accounts or incubate the accounts for committing fraud at a later point in time when it can go undetected. Fake accounts can lead to further issues if they are created to launder money or store stolen funds obtained through other types of fraud.

Second, businesses need to protect their customers from account takeovers, [or ATOs] — a form of fraud perpetrated by criminals to gain illicit access to existing accounts. The risk in this case for crypto exchanges is that users' tokens and funds stored in eWallets could be drained and sent overseas to false accounts controlled by the fraudsters or cashed out by other means.

ATO attacks can be committed using a variety of methods aimed at obtaining or guessing customers' login credentials. Such methods include credential stuffing, where batches of stolen usernames and passwords are injected into website forms using standard web automation tools; credential cracking, where brute force is employed to guess an account's password once the username is discovered; credential theft using keylogging, man-in-the-browser or other techniques; and session hijacking, a type of attack where a computer session key is attacked to gain unauthorized access to information.

In addition to account fraud, companies launching new services or entering new markets often face increased difficulty catching fraud because of the lack of historical data available to their fraud teams. Legacy fraud strategies rely too heavily on labeled data sets and require extensive historical knowledge to get up and running, which is simply not feasible in these situations. Fortunately, technology — especially unsupervised machine learning — can make a world of difference here.

What is the most significant difference between cryptocurrency fraud and other, more traditional forms of fraud, and how can consumer awareness be improved?

I mentioned that fraud attacks targeting crypto service providers are very similar to those that target other account-based services in some respects; however, there are some relevant differences that make criminals more likely to target firms offering these innovative services.

The first one is related to the ease of dissociation between the ownership of a cryptocurrency token and a real identity. Some experts point out that cryptocurrencies are not entirely anonymous given the advanced traceability offered by most blockchain protocols; however, even if transactions are traceable, this does not mean that they are tied to identities in the blockchain. A good term for this is that most crypto transactions are pseudonymous.

This contrasts with bank and other traditional transfers where, as long as funds remain in the financial system (i.e., are not cashed out), every transaction should be associated with the identities of all the parties involved — at least in theory. In the context of fraud, this means that cryptocurrency tokens obtained illicitly (e.g., by draining accounts after a successful takeover) can be moved between different accounts and ultimately used for the benefit of the criminals stealing them. The process of tracing these transfers and investigating illicit activities is more complicated should an audit be performed by companies or authorities.

A second difference lies in the irreversible nature of blockchain transactions, which in all senses is a feature of blockchain, not a bug. In fact, many users prefer cryptocurrencies over digital fiat transactions precisely because of the irreversible nature of the former and the true real-time payment possibilities that this unlocks. But for fraudsters, this means that once tokens are stolen and moved to an account under their control, they can sleep calmly, knowing that there's little or no recourse for the legitimate owners of those funds.

A third difference lies in another feature of blockchain protocols. Unlike digital fiat transactions that are governed and performed by central authorities, the decentralized nature of most blockchain protocols means that cross-border transactions are practically unlimited, with very little differentiation between sending funds to a person next door and sending them to a person on the other side of the world. All it takes in some instances is sharing the private and public keys to cold wallets over the phone, and funds can be made available anywhere.

All in all, these differences mean that companies currently offering cryptocurrency products and those seeking to enter the market should build … account security into their systems from day one.

What are some punctual recommendations to stop the kinds of attacks that you previously mentioned? How important to preventing fraud is users educating themselves and understanding cryptocurrencies and potential forms of fraud?

The crypto space is fascinating: Companies innovate daily, and users are enthusiastic about transforming finance. It is paramount that the few bad actors are weeded out to stop them from tarnishing the reputation of so many good innovations and loyal users.

First, FIs and FinTechs can stop account opening fraud by recognizing that identity validation measures are not enough to solve such a complex problem. When an account is opened solely based on whether or not the applicant provided an identity … that can be validated with a credit bureau, companies might be taking fraudsters' words at face value and neglecting to use evidence to truly single them out from good customers.

Fortunately for everyone — but criminals, of course — technology has come a long way and businesses can now spot fake accounts and block them before they inflict any damage. Early detection Is critical, and advanced fraud strategies should detect criminal activity in real time and before accounts are authorized, stopping the process before any damage occurs. Teams can leverage [unsupervised machine learning] to holistically analyze digital fingerprints, metadata and more to enable accurate decision-making — even with limited information.

On the other hand, ATO prevention requires a holistic approach where users and companies promote account safety in tandem. Companies should promote password best practices to make things [more difficult] for fraudsters, including deploying strong password requirements and educating users on good password hygiene. This implies changing passwords regularly, not recycling them across sites — especially with the same username — not sharing them with others and not writing them down.

Multifactor authentication can be effective, but its drawbacks need to be considered. Specifically, [multifactor authentication] introduces a substantial degree of friction to customer experiences, which can lead to user attrition. Therefore, companies should look carefully before implementing two-factor authentication measures and consider only requiring them for certain events (i.e., very large transactions) or for situations where an account takeover attack is suspected.

Thankfully, other options exist. Machine learning is especially useful to prevent[ing] takeover attempts. Instead of using high-friction authentication measures to stop ATO attempts, advanced strategies use [artificial intelligence] to analyze web session logs, cross-account linkages, digital fingerprints, profile details and account behavior to surface even the most stealthy fraud patterns without damaging the [user experience] for good customers.

Last but not least, companies launching new products or entering new markets where they possess limited information can leverage unsupervised machine learning to embed fraud prevention into their products from day one. Instead of relying on labeled datasets and extensive model training, advanced [unsupervised machine learning] techniques can stop fraud from day one by surfacing the connections between all the transactions, logins, accounts [and so on], and uncovering patterns that are invisible to the naked eye. This makes a world of difference in the fight against fraud.

PYMNTS Intelligence

The Growing Interest In **Cryptocurrency And Its Accompanying Risks**

While 86% of U.S. consumers are aware of cryptocurrency, its actual ownership or use remains relatively uncommon, with just 16% of consumers saying they have ever invested in, traded or otherwise made use of it. Interest in cryptocurrency is growing, however, and 38% of U.S. consumers believe the digital currency will have widespread acceptance for financial transactions within a decade.

This growing interest also means more opportunities for scammers. Growth in digital fraud is nothing new, but cryptocurrency fraud is unique by virtue of the combination of technologies and irreversibility involved in most protocols. Unlike checks or fund transfers, once most tokens have changed hands, the transaction cannot be canceled or reversed. Unlike hard currency, cryptocurrency cannot be physically locked away and is much easier to move, even in large quantities.

This month, PYMNTS examines the current state of the cryptocurrency space as well as the risks and rewards it holds.

CRYPTO AS A TRANSACTIONAL CURRENCY

Recent research from Mastercard found that 93% of North American consumers plan to use cryptocurrency or other emerging payment technologies within a year. A recent PYMNTS report revealed that even among those who originally purchased cryptocurrencies as an investment, nearly 63% would be highly interested in using cryptocurrency to make online purchases that are more private or secure than ordinary transactions.

FIGURE 1

Cryptocurrency owners' interest in using the digital currency in select ways

Share of cryptocurrency owners who are "very" or "extremely" interested in using cryptocurrencies in select ways, by current usage

Source: PYMNTS.com | Autopay The Cryptocurrency Payments Playbook

Privacy and security are not the only motivations for using crypto as a currency. Among consumers who would use cryptocurrency to purchase real estate if given that option, 40% said their motive would be to eliminate "middlemen" from the transaction. Efficiency and lower transaction costs are other significant motivators for many consumers. Nearly 40% would pay for streaming services with cryptocurrencies for more efficient online payments, and more than 35% would use cryptocurrencies to pay for streaming to have lower online transaction costs.

Already, significant sums of cryptocurrency are being exchanged for goods and services. Visa reported $1 billion in transactions globally with its crypto-linked cards during the first six months of 2021. Among millennials, 75% said the only thing holding them back from using cryptocurrency is a lack of understanding of how it works.

FRAUD AND REGULATION IN THE CRYPTO SPACE

While the cryptocurrency space is beginning to come under greater scrutiny from regulatory agencies, the lack of regulatory certainty leaves opportunities for scams and fraud. The general public's relative unfamiliarity with crypto makes it much easier for scammers to create their own exchanges expressly to scam users. Such exchanges may deny withdrawals, charge exorbitant fees or simply take users' crypto assets and disappear. Other scammers target well-established or reputable crypto exchanges with attempts to manipulate trading volumes.

Multiple established exchanges have closed — either temporarily or permanently — due to a proliferation of fraudulent transactions or other scams. Regulators are often stymied by the pseudonymous nature of crypto transactions, with even the best efforts to trace transactions failing to reveal the parties involved. Regulatory action is further complicated by the ease with which cryptocurrencies can be used in cross-border transactions.

FIGURE 2

Reasons consumers would be likely to purchase select products using cryptocurrency, if available

Reasons consumers would be likely to purchase select products using cryptocurrency if available, by product category

	N	To make my financial transactions more secure	To make my financial transactions more private	To make online payments more efficient	To eliminate "middlemen" from my transactions	To pay lower online transaction costs
Streaming	1446	34.2%	32.9%	39.5%	27.0%	35.2%
Online gaming or gambling	1092	36.2%	38.7%	34.8%	28.8%	35.0%
Entertainment and media	1253	35.4%	33.5%	39.4%	28.0%	36.0%
Real estate	1214	40.2%	39.8%	33.8%	40.0%	33.1%
Education/training services	999	37.6%	35.9%	35.4%	32.9%	34.0%
Groceries	1461	32.0%	31.7%	33.3%	25.6%	31.3%
Professional services	1172	36.9%	39.8%	36.3%	32.7%	34.1%

Source: PYMNTS.com | Autopay The Cryptocurrency Payments Playbook

There have also been many high-profile cryptocurrency heists that have occurred. One attack on the decentralized finance (DeFi) platform Poly Network netted the attacker more than $600 million in cryptocurrency. The attacker did not require accomplices, vehicles or a duffle bag to stuff with cash, as they stole every digit of that $600 million electronically — and it was also untraceable. Bad actors are estimated to have stolen $14 billion in cryptocurrencies during 2021.

Not all crypto exchanges and providers are equal, and DeFi platforms are known to be susceptible to security risks to a greater degree than others. Some services now employ biometrics to help secure users' assets while also requiring authorization protections such as digital identities and wallet ID tokens. There are other security options, such as MFA, which requires users to confirm through multiple devices or methods that they are who they say they are. Such measures are only as strong as the platforms behind them, however, and attackers have defeated MFA by simply going around it.

The potential pitfalls of cryptocurrency are many, but consumer interest in it is not going away. Financial services companies and regulators must continue to adapt technologically and operationally to ensure that cryptocurrency matures as a stable, reliable financial tool.

NEWS & TRENDS

CRYPTOCURRENCY **GROWTH AND GROWING PAINS**

HIDDEN FUNCTIONS REVEAL N26 APPEARS TO BE PLANNING IN-APP CRYPTO TRADING

German neobank N26 could be planning to offer customers cryptocurrency trading through its mobile app, new research revealed. The XDA developers' mobile software development community discovered the potential offering by decompiling N26's Android Package Kit (APK) file, which included hidden functionalities related to cryptocurrency trading. Fellow neobank Revolut already offers similar functionality through its mobile app and permits users to store and convert various currencies, including euros, British pounds and U.S. dollars. The app supports transactions in multiple cryptocurrencies as well.

The decompiled APK information indicates that future cryptocurrency trading through N26 would be facilitated by a partnership with cryptocurrency trading platform Bitpanda. The code shows the implementation of full transparency regarding any fees involved as well as the functionality to enable a clear portfolio overview. This incident is not the first indication that N26 has been looking to facilitate cryptocurrency trading through its mobile app, and it may have been exploring this ability since 2021.

COINBASE'S QUARTERLY VOLATILITY DEMONSTRATES NEED FOR DIVERSIFIED PRODUCT OFFERINGS

Cryptocurrency operator Coinbase had a successful 2021, but that growth may be slumping by equally impressive margins this year. Coinbase's year-over-year trading volume was up 515% by Q4 2021, accompanied by a 67% quarter-over-quarter growth in trades. At the same time, Coinbase's number of monthly transacting users was also up, growing 307% from 2020 and 54% from Q3 2021. These factors combined give Coinbase a 102% net earnings increase quarter-over-quarter and a 375% increase year-over-year.

Q1 2022 has not been nearly as rosy, however, and Coinbase has announced several plans to diversify its cryptocurrency offerings to compensate. Coinbase is predicting a quarterly trading volume decline as well as a slump in monthly transacting users. Some of Coinbase's efforts to adapt include pushing the use of crypto as a currency, such as with its Coinbase Card, which consumers can use to make crypto-based purchases in the physical world. Coinbase is also pushing crypto-backed loans and has launched a fund-transfers product from the U.S. to Mexico.

UK CRYPTO PROVIDERS CLOSE SHOP AHEAD OF REGULATORY DEADLINE

New pressure from the United Kingdom's Financial Conduct Authority (FCA) may be causing some cryptocurrency trading providers to close up shop in the country. The move by some firms to shutter their U.K. operations follows the FCA's notification to multiple cryptocurrency providers that they are likely to be rejected for permanent registration in the FCA's anti-money laundering registry. The FCA previously created a temporary version of the register to accommodate cryptocurrency providers while further considering the situation. Operators on the temporary register had until the end of March to win approval from the FCA for inclusion on the permanent register. Cryptocurrency operations not added to the permanent register will have to close regardless, so some that believe there is a low chance of being accepted have closed early to reduce the risk if they waited for official confirmation of their rejection.

INTERCEPTING **FRAUD IN THE DIGITAL SPACE**

CRYPTOCURRENCY-RELATED SCAM REPORTS AND CHECKS ROSE SIGNIFICANTLY IN 2021

In addition to efforts to secure the cryptocurrency space against money laundering, the U.K.'s FCA has also been tracking an increase in scams that specifically target consumers using cryptocurrencies. Out of approximately 16,400 possible scam reports the agency received between April 2021 and September 2021, 3,000 were cryptocurrency-related. The most-reported scam involved fraudsters attempting to push targeted consumers to purchase worthless, overpriced or nonexistent shares or bonds over the phone. Reports of cryptocurrency scams were the second-most common type reported throughout the year, peaking in June, and reports of cryptocurrency scams were up 14% from the previous six-month period.

As reports of cryptocurrency scams were on the rise, so was concern among U.K. consumers that they did not fall victim to scammers. The FCA maintains a ScamSmart Warning List that consumers can use to check whether a purported investment opportunity has been flagged as a scam. Use of the tool from April 2021 to September 2021 to check on potential cryptocurrency scams rose 49% from the previous six-month period, becoming the most checked item on the list.

FI FRAUD PREVENTION MUST STRIKE BALANCE WITH USABILITY, SURVEY FINDS

A recent survey of U.K. consumers showed that FIs could lose customers if they cannot create a balance between robust security protocols and user experience. This is compounded by a lack of awareness among those consumers regarding the technical sophistication of some forms of fraud. While 26% of U.K. consumers said they were concerned about account takeovers and scammers opening fraudulent accounts in their names, just 6% were concerned about authorized push payments fraud or being tricked into sending a payment to a bad actor.

At the same time, respondents indicated that they would consider switching FIs if the security protocols in place were too burdensome. Nineteen percent said their biggest irritation with FIs occurs when fraud prevention systems block legitimate purchases, and 35% said they would switch to a different provider if an online transaction was incorrectly declined three or more times.

The cryptocurrency ecosystem

PYMNTS.com | DATAVISOR

Cryptocurrency is already in use as more than just a speculative investment, such as for those sending cross-border remittances, but lack of knowledge and security concerns are limiting the speed of adoption for both consumers and business decision-makers.

Reasons for not purchasing cryptocurrency.

Despite its growing popularity, many consumers are still hesitant to purchase cryptocurrency, but their reasons vary.

73%
Lack of knowledge

33%
Not mainstream or accepted enough

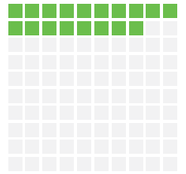
25%
Cryptocurrency value is too volatile

22%
Do not view it as a good investment

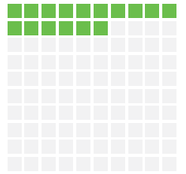
Factors informing FIs' blockchain and cryptocurrency strategies

As FIs make decisions regarding cryptocurrencies and blockchain, various factors within their organizations inform strategies, not the least of which is data security.

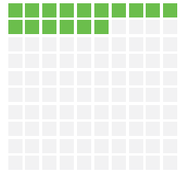
18%
Strength and weakness of current internal infrastructure



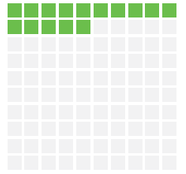
16%
Potential for better data security



16%
Risk of new business model disruptions



15%
Potential for capturing real-time reference data



Most common method for recipients to receive cross-border payments

Consumers make cross-border payments in several ways, including cryptocurrency, and how consumers actually receive those payments can vary among recipients, even when they are using the same payment method.

Money received directly to a BANK ACCOUNT:

47%	Average
52%	Bank transfer
35%	Cryptocurrency

Money received directly into a MOBILE WALLET:

30%	Average
30%	Bank transfer
46%	Cryptocurrency

Cryptocurrency Payments Playbook. PYMNTS.com. 2021. https://www.pymnts.com/wp-content/uploads/2021/07/PYMNTS-Cryptocurrency-Payments-Playbook-July-2021.pdf. Accessed March 2022.
The Corporate Treasury Shift. PYMNTS.com. 2022. https://www.pymnts.com/wp-content/uploads/2022/01/PYMNTS-The-Corporate-Treasury-Shift-January-2022.pdf. Accessed March 2022.
The Digital Currency Shift. PYMNTS.com. 2021. https://www.pymnts.com/wp-content/uploads/2021/09/PYMNTS-Cross-Border-Remittances-Report-September-2021.pdf. Accessed March 2022.

DIGITAL FRAUD

TRACKER®

ABOUT

PYMNTS.com

PYMNTS.com is where the best minds and the best content meet on the web to learn about “What’s Next” in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

DATAVISOR

DataVisor’s mission is to build and restore trust online. It partners with the largest financial and internet properties in the world to protect them from a wide array of attacks, including fraud, abuse and money laundering. The company’s unsupervised ML-based detection solution detects attackers without needing training data, and often before they can do damage.

DataVisor is made up of a team of world-class experts in Big Data infrastructure and ML. It builds advanced algorithms to fight the world’s most sophisticated online attackers.

We are interested in your feedback on this report. If you have questions or comments, or if you would like to subscribe to this report, please email us at feedback@pymnts.com.

DISCLAIMER