DEPTH. FOCUS. SERVICE.

MERCATOR ADVISORY GROUP

MODERNIZING FRAUD PREVENTION WITH AUTOMATION, MACHINE LEARNING, AND A GLOBAL NETWORK

An escalating commerce climate requires a new approach to fraud prevention.

A Mercator Advisory Group White Paper Sponsored by Forter

FORTER®

June 2020

Contents

Introduction—Fraud on the Rise ***3***

Consumers Looking for Instant Gratification ***3***

The Common Approach to Fraud Prevention ***3***

Pitfalls of the Traditional Approach to Fraud Prevention ***5***

Modernizing Your Fraud Prevention System ***5***

Fraud Prevention Capabilities Your Business Needs ***6***

An Integrated Platform Protecting Across the Entire Purchasing Journey 6

Understanding a More Complete Story 6

Streamlining the Customer Experience and Offering New Services 7

Global Network ***8***

Fraudulent Activities 8

Legitimate Consumer Behaviors and Interactions 8

Identity Linking 9

Machine Learning for Greater Accuracy ***9***

Supervised Machine Learning 9

Unsupervised Machine Learning 10

A Hybrid Approach: Man and the Machine 10

Advanced Fraud Analytics ***11***

Tailored Fraud Prevention Models 12

The Way Forward ***14***

Endnotes 15

Introduction—Fraud on the Rise

In 2019 Visa reported that 4.5% of orders for digital goods and 3% for physical goods were rejected due to suspicion of fraud. Due to payment fraud on domestic orders, merchants lost 2.5% of e-commerce revenue on digital goods and 1.3% on physical goods. [i]

With stolen data freely available on the dark web, cyber-criminals can take over accounts, open new accounts, steal valid identities, or create synthetic ones. They can monetize by using unauthorized credit card details to make purchases or by redeeming rewards points out of loyalty accounts.

It's a lucrative business. So it's no surprise that fraud is rising not only in the total number of attacks but in the variety of fraud vectors.

Cybercrime is projected to cost the world $6 trillion annually by 2021.[ii]

Vectors of fraud and abuse are expanding and growing. Account takeover attacks are growing increasingly sophisticated. Fraud and abuse pain points are now no longer only limited to professional online criminals. Even merchants' customers are getting in on the act through policy abuse, wherein they exploit loopholes in coupon programs, welcome benefits, referral bonuses, and loyalty rewards for their own benefit.

Cybercrime has become more sophisticated. Fraudsters are using a broad range of tactics, such as phishing, pharming or whaling, identity theft, account takeover, card-testing friendly fraud, affiliate fraud, and abuse of coupons, discounts, and refunds. They're using automation to launch large-scale attacks, and they're colluding to defraud online businesses in new ways.

Consumers Looking for Instant Gratification

Consumer expectations of their favorite brands are also on the rise. Merchants must be prepared to contend with this new norm of customer experience where instant gratification, immediate fulfillment, and heightened personalization are expected, no matter how or where customers shop. Merchants are competing for customer lifetime value (LTV), which means they need to win at every interaction across the customer journey (from login to sign up to coupon and loyalty point redemption)—not just at the point of transaction. This requires a sophisticated and automated system that not only makes the payment process seamless and simple, but likewise minimizes friction for consumers during coupon code redemptions, return requests, and expedited shipping requests.

The Common Approach to Fraud Prevention

Confronting a growing and evolving fraud problem, many merchants started by implementing point solutions to address specific concerns. For example:

- **Rule-based tools** flag and block actions or users based on fixed attributes such as a mismatch between data listed on the credit card and the email username.

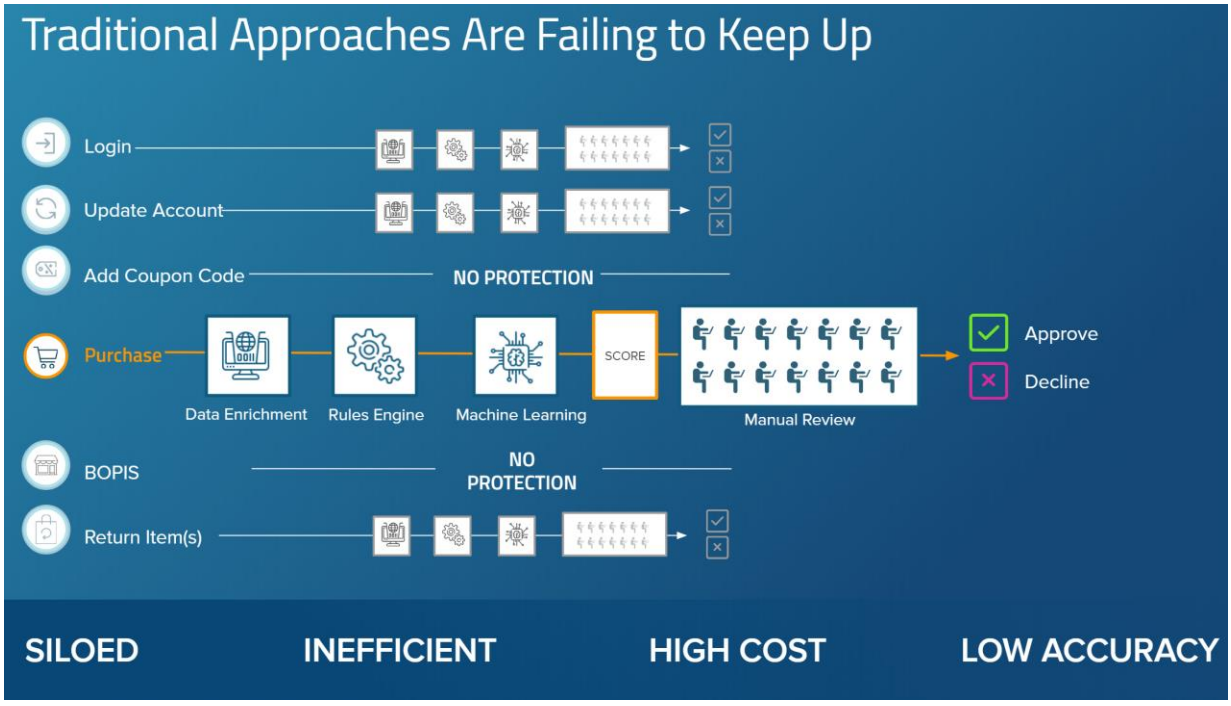
- **Data enrichment tools** are often added to refine these rules, such as data enrichment tools to collect additional information based on a specific data point (e.g. more information about an email address).

- **Out-of-the-box machine learning tools** add a layer in the attempt to isolate specific fraud behaviors and scale fraud prevention efforts.

- **A manual review** process handles questionable transactions, with workflow often managed on an exception basis and prioritized based on agent availability.

- **One-off, situation-specific tools** are added to protect new fraud vectors or to seal any gaps or misses that may have occurred in previous cases or contexts. However, note that adding a tool to solve just one type of problem, such as account takeover attempts or attacks, will not protect the system from other forms of fraud or possible vulnerabilities.

Today's dynamic e-commerce climate, shifting consumer demands, and evolving fraud environment require more sophisticated and proactive fraud prevention than legacy approaches. While siloed, legacy approaches once were sufficient, current transaction volumes and the variety of interactions (both legitimate and fraudulent) underscore gaps and weaknesses of traditional approaches.



Pitfalls of the Traditional Approach to Fraud Prevention

Current approaches to fraud and abuse prevention create the following weaknesses for enterprises:

- **Lower accuracy by focusing on transactions, not digital identity.** Most legacy solutions focus on the transactions rather than understanding the constant reputation of the digital identity behind them. Transaction behavior can be manipulated through proxies or breached personal details. However, people aka digital identities are more consistent, they rarely change their behavior, whether they are good or nefarious actors. Looking only at transactions rather than one's digital identity yields inaccurate results and lost revenue. Fraud decisions are made using only a subset of relevant data for each use case. This can lead to an inconsistent experience for the customer often resulting in increased false positives or friction for legitimate users.

- **Gaps create easy targets for fraudsters.** There is a lack of coordination among the different tools which is exactly the type of situation fraudsters look for, since it creates gaps they can exploit. Information is siloed which allows instances of fraud and abuse to slip through the cracks and ultimately results in increased fraud costs.

- **Scalability.** Siloed solutions that were not built to work together are extremely difficult to scale, especially as business requirements change during peak periods, flash sales, or as new fraud attacks appear. Ongoing manual processes require higher operational costs to maintain.

- **Keeping up with new forms of fraud.** Legacy systems that rely on rules or manual review teams are reactive rather than proactive, meaning the business will not be protected against new and evolving fraud and abuse trends.

- **Risk avoidance.** Due to fear of risk and the inability to amply protect their business, merchants avoid new products, offerings, and growth into new markets.

- **Data exposure.** Using multiple tools is more likely to expose customers' sensitive and personally identifiable information (PII). This can trigger privacy and compliance issues.

Modernizing Your Fraud Prevention System

Businesses should look to a single, comprehensive fraud prevention platform capable of assessing trust at every point of interaction in real time – from login to coupon redemption to delivery and returns experiences. A best-in-class solution will use data from across industries, enterprises, geographies, and types of fraud attacks, allowing businesses to:

- **Increase top-line revenue** by accurately identifying legitimate customers and approving more transactions. Reduce false positives by up to 90%.

- **Grow without risk** to deliver new programs in new markets without worrying about fraud and abuse.

- **Proactively identify new fraud threats and accurately catch fraud to** minimize direct fraud losses and the potential of tarnished business reputation. Reduce chargeback losses by up to 90%.

- **Digitally transform** to deliver a consistent, trusted, and highly personalized experience via digital channels, allowing customers to engage with their favorite brands wherever and however they choose.

Fraud Prevention Capabilities Your Business Needs

Mercator assessed the fraud environment and prevailing fraud technologies to ask, "What does it take to empower enterprises to answer two central questions:"

"Do I know the digital identity behind this transaction to evaluate whether they are a legitimate buyer?" and **"Can I trust this digital identity's behavior on this site?"**

This white paper identifies five essential capabilities for a modern fraud prevention system that allow the merchant to answer the two questions above:

- An integrated platform that provides protection across all customer touch points in the purchasing journey

- A global data network

- Machine learning for greater accuracy

- Advanced fraud analytics

- Tailoring of fraud models to an individual enterprise

An Integrated Platform Protecting Across the Entire Purchasing Journey

An effective fraud prevention strategy requires having the best data sets connected in one place. An integrated and comprehensive fraud prevention platform connects and analyzes fraud data across all touch points in the customer purchasing journey, not just at the point of transaction.

Understanding a More Complete Story

True understanding of consumers, their actions and their accounts, comes from monitoring and evaluating every step they take, and how they are connected to other users on your site. Rules systems miss out on consumer activities at different points in the purchasing journey and fail to see how these details can help build a clearer picture of a consumer's digital identity within their business system.

> To solve fraud and abuse problems requires the continuous inspection of a customer throughout the purchasing journey on a business's website.

Fraud decisioning cannot depend on a single data point. All details and data points must be reviewed to assess the trustworthiness of the identity behind the transaction. A simple parallel would be how one would approach scouting a player for a sports team – Do you read stats from the last game or from the entire season? Do you just watch him/her on video? Do you interview his/her coaches and teammates? You would do these things while also taking into consideration other less obvious elements like: What is his/her weight room or training regimen?

Much in this same way, a fraud prevention system must consider the story, factors, and reputation behind the behaviors it sees to view the data within the proper context depending on a variety of coexisting factors. Is this a true, complex story, or a false one?

Every touch point in the consumer journey from the initial visit to login, coupon use, checkout, returns, and beyond, must be integrated into the fraud decisioning process. By aggregating data from across all of these touch points, businesses are armed with a richer picture of consumer behaviors and are better able to distinguish legitimate activities from fraudulent ones. For example, to detect different activities of the same fraudster or fraud ring, the system must be able to connect different transaction attempts and block the large (or small) scale attack.

Streamlining the Customer Experience and Offering New Services

Accurately identifying legitimate buyers means that businesses can remove unnecessary friction across different touch points, streamlining their path to checkout. Rather than good customers being pushed through multiple instances of authentication, businesses will be able to offer "1-Click" type of checkout processes to their verified customers.

Friction based on risk means the system will be able to maximize sales and ensure consumer experience contains the minimal and most suitable necessary friction (e.g. when to apply 3DS, when a customer should present an ID / credit card when picking up products in-store). By streamlining the entire customer buying journey, enterprises will be able to increase the lifetime value (LTV) of their best and most valued customers.

To provide a best-in-class customer experience, enterprises need to digitally transform their businesses to meet growing consumer demands. By looking beyond just the point of transaction and protecting touch points across the buyer's journey, enterprises can offer new products such as loyalty programs, flexible returns policies, and private label credit cards, areas they may have once considered to be too high risk for fraud.

Whether a consumer is signing up, logging in, changing their financial information, using loyalty points, or taking any other action associated with their account, an integrated fraud prevention platform that monitors the full journey will analyze all of the factors of their behavior and actions and compare them to past behaviors and actions, known behaviors associated with similar profiles, relationships with other accounts, etc. It will identify, in real time, any activities which appear to indicate that fraudulent or non-compliant activity (i.e. acting against merchant policies) is taking place. This comprehensive view allows the integrated platform to help protect all merchant customers.

By taking into consideration the entirety of the customer journey, businesses will have a more unified perspective of the digital identities in their ecosystem and be able to proactively protect against emerging forms of fraud and policy abuse. Merchants will also be able to more rapidly digital transform their business, augmenting

omnichannel customer experiences and offerings (i.e. Buy Online Pickup In Store (BOPIS) or Buy Online Return In Store (BORIS)). This will allow them to deliver a consistent, trusted, and highly personalized experience via digital channels, and allow customers to engage with their favorite brands wherever and however they choose.

Global Network

Fraudsters move fast, so it is essential for businesses to keep ahead of current fraud trends and methods of attack. Integrating fraud data from merchants around the world enables:

- A more comprehensive view of fraudulent activities
- A foundation of legitimate consumer behaviors and interactions
- The ability for the fraud platform to link between identities

This white paper focuses on Forter's Global Network, which aggregates data from multiple merchants across verticals and geographies. Consumer behavior changes fast, and fraudsters move even faster. To keep up with today's fast-changing world, it is essential to leverage a wide set of data across geographies, touch points, industries, and clients. This data is particularly valuable when assessing transactions for infrequent customers or those with only a thin behavioral data file.

Fraudulent Activities

As part of a fraud prevention Global Network, enterprises benefit from the knowledge and insights gained from across other enterprises, in real-time. If a new fraud technique is attempted against one client, the rest of the network will be protected against that fraud technique. Likewise, if the system has seen the legitimate user in the network in the past, it now can identify the fraudster's attempt to use the legitimate user's identity and credentials, and block it within the first attempt. As a result of this "Network Effect" or the ability to see a wider set of data across enterprises, each business benefits from a wider cross-network inoculation against all fraud types observed across clients in all geographies and industries. This capability is critical when dealing with fraud rings that launch attacks across a broad set of enterprises that span geographies and verticals over a short period of time. This Network Effect ultimately improves an enterprise's ability to more accurately protect their business and customer accounts from emerging fraud and abuse trends.

Legitimate Consumer Behaviors and Interactions

The Global Network also provides a more accurate view of *legitimate* consumer behaviors. Interactions from across the network are taken into account and can benefit all members of the Global Network. Without these network-wide insights, each enterprise only has visibility into a subset of their own data and legitimate activities and trends. This narrow view leads to falsely declining good customers. Through a Global Network, enterprises can benefit from what trends and behaviors the system has learned elsewhere, allowing them to have a more accurate picture of legitimate consumer behaviors from across the network.

Identity Linking

Linking is key to using a robust global network of data. Identity linking technology allows connections and relationships to be traced between identities even when no single datapoint is shared. The ability to find similarities among people and events and link them across a global database, enables the solution to differentiate between good and bad actors and note shifts in behavioral elements that would otherwise be indistinguishable for legacy systems with siloed data.

The ability to link and connect identities benefits the system in two ways:

- **Bad actors.** If the system only uses static data, it is much easier for a fraudster to hide. Elastic linking (or the ability to connect identities based on similar behaviors/interactions) is a better way to detect bad actors that are trying to hide all of their connections.

- **Good actors.** Detecting the connections between colleagues or family members through elastic linking will enable the ability to provide an excellent experience to connected accounts in the same way you would want your lifetime value customers to experience.

Machine Learning for Greater Accuracy

Machine learning is also key to a successful fraud prevention system. Full automation, with real-time approve/decline decisions and notifications at any point in the customer purchasing journey, would simply not be possible without it. Rules and scores cannot keep up with today's fast-moving online criminals, who already use automation and basic machine learning themselves.

Machine learning is at the core of many fraud prevention platforms because of its unsurpassed ability to recognize patterns in massive amounts of data, even complex fraud behaviors, and to use that learning to assess current behaviors in real time.

Supervised Machine Learning

This approach uses historical data about known fraud incidents to “train” the model to recognize fraud in new data. This approach accurately detects fraud types that have already been identified and can be categorized. The challenge here is specifically around having enough tagged data and the quality of the tagging. It is near impossible to have enough fraud data upon which to train the models. This includes a low number of chargebacks, high numbers of biased declines, many fraud cases that are actually repeat fraudsters (so the training is on this fraudster rather than on the fraud itself), the data as a reflection of what things *used* to look like, and the model not being able to identify new fraud trends or regular changes in the world. Such things that include new operating systems, new browsers, new products the merchant may be selling, or new markets they expand into.

Unsupervised Machine Learning

This approach analyzes all transactions to establish statistical bounds associated with normal transactions – and then recognizes new transactions that stray too far from the statistical normal path and considers them suspicious. This approach can detect new forms of fraud, but it delivers high false-positive rates. In addition, new forms of fraud that occur while the model is being "trained" will become part of the baseline and not flagged as abnormal, thereby creating a false negative event.

A Hybrid Approach: Man and the Machine

Machines require "big data" — huge data sets with many examples of a trend. Fraud is often characterized by "small data." Letting many examples of a new fraud technique through is detrimental because the machine doesn't have enough instances yet to learn to block it. Through ongoing research into consumer buying patterns, behavioral analytics, payment trends and the fraudster ecosystem, advanced fraud analytics and expert human curation can turn insights gleaned from their analysis into attributes that the machine can use to stop fraud in real-time.

Next generation fraud prevention takes a hybrid approach that uses supervised and unsupervised machine learning, coupled with human expertise and ongoing research. While rules, policies and blacklists/whitelists once formed the base of a fraud system, ML models are now the base. Legacy systems of rules and policies resulted in controls that are relatively static, reactive to cases of fraud that have occurred in the past, and easy for fraudsters to test and circumvent. Understanding real-world problems and how they may impact fraud models and business needs requires a combination of human expertise and machine learning.

> Ultimately, machine learning is only a tool. It is only as good as the data it has to work with and the experts who are able to continually refine it. It needs human intervention as machine learning alone is not enough for accuracy.

Without human expert curation, machine learning results in the following deficiencies:

- **Limited data.** There might not have been enough data in the training set to let simple machine learning extract all relevant information and tell the whole story.
- **Failing to protect against evolving fraud trends.** Because vectors of fraud and abuse are constantly changing, the training data set on which the machine learning algorithms were built might not reflect all fraud and abuse use cases that could be impacting an enterprise in the current environment. Additionally, fraudsters are intelligent adversaries, which puts the problem of fraud into the realm of game theory. Loopholes in the defenses that did not manifest in the original training set could still be harmful if found by fraudsters.

- **High false positives for new business initiatives.** Due to limited data, enterprises will end up having fraud prevention systems that will actually reject legitimate buyers. This will limit business' ability to expand into new products, offerings, and new markets successfully.

It therefore requires human expertise, industry knowledge, and ongoing curation to build machine learning and operational processes that can resolve these deficiencies, such as:

- **Attribute curation**. Finding new data points or data combinations that are efficient in detecting certain attacks and then adding them to the models.

- **Gap analysis and story models.** Investigating outliers and anomalies so that inconsistent data doesn't end up skewing the model.

Machine learning along with the research and insights added to the models allows enterprises to enter new markets, new fields, and leverage existing data in a much more accurate way. This approach accommodates events that are not exactly identical to behaviors that may have been previously seen, which maximizes the sample size.

Without this sophisticated curation, machine learning will become less efficient over time and lose its key differentiation. For ML to work well, it needs hundreds of examples of fraud for specific use cases allowing for grouping or clustering into behaviors that describe real behaviors. That's why most advancements in machine learning remain the focus of data scientists paired with advanced fraud analytics, to stay aware of the latest discoveries and trends in global online fraud.

Advanced Fraud Analytics

Forter staffs an entire research team—dedicated fraud experts and data scientists. These individuals:

- Proactively research and uncover new fraud trends

- Identify behavioral patterns in the data

- Actively adjust the linking models and decision models

- Identify attack vectors

and then engineer ways to identify and stop them.

This team conducts global research on fraud trends and feeds these insights into the machine learning platform. The researchers monitor fraudster marketplaces and forums and bake their insights into the models. Rather than simply place raw data into a model, Forter's researchers curate the data inputs to build a real-world story. For example, if you were to have an IP for a country (Peru) and the card country (Israel) for a particular transaction, you could just drop them into a ML model. This would likely yield a false positive, and negatively decline a good

customer. With curation analysts engineer features that assist the model in understanding a more complete story around the data: This user is likely an Israeli tourist on a trip in Peru.

This advanced fraud research is important in ensuring that fraud prevention is always up-to-date and as accurate as possible – shared for the benefit of Forter Global Network members.

A next generation fraud system will conduct analysis that derives deep insights from the data. For example:

- **Cyberintelligence.** This form of intelligence powers ability to identify fraud rings or repeat fraudsters using new details or devices. Identity-linking technology finds hidden connections even when entities don't have a single data point in common and identifies means of identity manipulation. This helps to provide additional depth to analysis by indicating whether users are concealing their location, and also their true location — and whether that difference is legitimate or a sign of fraud. This capability adds particular value for understanding fraud in digital goods, such as e-tickets or gift cards.

- **Behavioral analytics.** Allow enterprise to identify behavior of the user on the platform, in order to identify the nature of the behavior, the probability of the user being a bot, or identifying suspicious browsing patterns. These behavioral indications later feed the linking models as well as the decision models and help to flesh out the identity behind the data points, ultimately enabling the system to understand when particular behaviors are atypical for a specific user or entity.

- **Tailoring and feedback.** Incorporating client feedback on an ongoing basis into the fraud prevention models means a uniquely tailored solution. In partnership, the system is continually updating, reacting to new data to become more and more tailored to each client's unique risk profile. (For more information, see Tailored Fraud Models).

Tailored Fraud Prevention Models

Every business is unique and has its own operational structure, product offerings, cost/revenue approaches, and risk appetite. Every one of these attributes changes over time as a result of conscious business decisions or new information that becomes available. An effective solution must support the risk management team to protect the business as it operates today and as it evolves, no matter the nature or pace of change.

Without this ongoing customization and tuning to the business's unique attributes, models will "drift" and become

less accurate over time. Patterns of behavior that were highly predictive in the past may be less predictive during times of change. Until the model is updated or retrained on new patterns, its results will be influenced by outdated algorithms.

Who should do the work of keeping models current? To yield the best results, a close partnership between the enterprises' in-house experts and an advanced fraud prevention provider is required. A partnership that combines the deep business knowledge in-house teams have with the visibility and depth and breadth of data an external

vendor provides will allow for a full understanding of the risks, fraud vectors, and needs of the business – all to better tailor the fraud models to the requirements necessary for the specific enterprise.

For example, advanced fraud prevention solutions build a custom risk model for each enterprise tailored to their:

- Risk appetite
- Geography
- Business Models, promotion and marketing efforts
- Product and service portfolio
- Desired customer journey / business policies
- Digital Initiatives (e.g. BOPIS / BORIS)

Tailoring the solution occurs using the enterprise's data and insights gleaned from the Global Merchant Network database. This process prevents fraud and abuse from migrating from one merchant to another.

An enterprise tailored model is built with the enterprise's historical data and then synchronized and adjusted on an ongoing basis to meet changing consumer behaviors, expectations, and the dynamic nature of fraud. Through regular meetings with the fraud prevention partner and direct self-reporting mechanisms, enterprises offer real-time feedback so their model is always current with changing business conditions, such as new products, promotions, or entry into a new market.

Benefits of a tailored model include:

- Dynamic, real-time trust decisions to reduce direct fraud losses and minimize costly operational overhead caused by account takeovers.
- Protection against policy abuse— where good customers take advantage of merchant policies. The enhanced detection and blocking of promotion, coupon, and referral abusers exploiting these benefits.
- Allowing enterprises to offer a unique customer experience by reducing friction for trusted customers or by allowing the business to provide special service to trusted customers that other platforms would deem "too risky."
- Identifying the most accurate balance for each specific merchants' acceptance rate and risk exposure, on all dimensions and verticals, while always adjusting it in accordance to the internal (merchant's goals and plans) and external (market trends, fraud trends) changes.

Continuous tailoring and feedback between the enterprise and the fraud prevention solution partner yields more accurate fraud decisions, even if the e-commerce climate shifts or business requirements expand. Effective fraud prevention should not be seen as a solution that, straight out of the box, will accurately resolve fraud amid shifting

business priorities. Rather, the platform must be constantly updated to reflect new attack vectors and changes in business operations. Choose a vendor that will create a custom risk model tuned to your data, unique business requirements, risk appetite, and feedback from the field.

The Way Forward

With rising consumer expectations and emerging vectors of sophisticated fraud and abuse, businesses need to be prepared to better protect themselves and their customers. Amid growing sophistication in fraud attacks, contending with abusive behaviors perpetrated even by good customers, and balancing the need to offer more streamlined customer benefit offerings, merchants have their work cut out for them. In order to strike the right balance between fraud and abuse prevention while ensuring a best-in-class customer experience and top line revenue growth, merchants need a next-generation fraud prevention solution. Working with a modern, integrated fraud solution platform that combines machine learning with human expertise provides the following core benefits:

- **Accurately distinguishes legitimate customers** from fraudsters, bots, or abusers through advanced analytics, a robust global data network, and machine learning continually tuned by fraud prevention experts.
- **Eliminates the need to manage multiple fraud tools and vendors** by using one integrated platform to cover the entire online customer journey, protecting against fraud and abuse across all customer touch points and minimizing the risk of data exposure and the range of fraud tactics.
- **Reduces costs and delays** by automating approve/decline decisions in real time without reliance on manual reviews.
- **Catches otherwise unknown patterns of fraud** by analyzing a depth of data resources from inside the company and across enterprises across the globe with a global data network.
- **Boosts approval rates, brand loyalty, customer trust, and revenue** by eliminating unnecessary friction and false positives in consumer transactions.
- **Scales as needed**, easing the go-to-market path in terms of computing capacity and fraud risk, so the enterprise can take advantage of new opportunities, markets, and offerings.

Furthermore, by switching from layered, siloed solutions to an integrated platform, an enterprise shifts its fraud prevention stance from reactively plugging gaps to proactively taking control over fraud mitigation. Enterprises can focus on improving the business, not worrying about fraud.

> With a modern integrated fraud prevention platform, the merchant's fraud team can proactively take measures to mitigate fraud and maximize the company's revenue opportunities while giving customers the brand experience they have come to expect in this age of immediacy.

Endnotes

i. Visa, *2019 Global e-commerce Fraud Management Report*, p. 36.

ii. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

About Mercator Advisory Group

Mercator Advisory Group is the leading independent research and advisory services firm exclusively focused on the payments and banking industries. We deliver a unique blend of services designed to help clients uncover the most lucrative opportunities to maximize revenue growth and contain costs. Advisory Services. Unparalleled independent and objective analysis in research documents and advice provided by our Credit, Debit and Alternative Products, Prepaid, Merchant Services, Commercial and Enterprise Payments, Emerging Technologies, and Global Payments practices. Primary Data. North American PaymentsInsights series presents eight annual summary reports based on primary data from Mercator Advisory Group's bi-annual surveys of 3,000 U.S. adult consumers to determine their behavior, use, preferences, and adoption of current and emerging payment methods and banking channels to help our clients identify and evaluate business opportunities and make critical business decisions. Two other Mercator survey series—Small Business PaymentsInsights and Buyer PaymentsInsights—each receive coverage in three reports annually. Consulting Services. Services enabling clients to gain actionable insights, implement more effective strategies, and accelerate go-to-market plans. Offerings include tailored project-based expertise, customized primary research, goto-market collateral, market sizing, competitive intelligence, and payments industry training. PaymentsJournal.com. The industry's only free, analyst-driven, online payments and banking news information portal delivering focused content, expert insights, and timely news.

About Forter

Forter is the leader in e-commerce fraud prevention, processing over $150 billion in online commerce transactions and protecting over 750 million consumers globally from credit card fraud, account takeover, identity theft, and more. The company's identity-based fraud prevention solution detects fraudulent activity in real-time, throughout all online consumer experiences.

Forter's integrated fraud prevention platform is fed by its rapidly growing Global Merchant Network, underpinned by predictive fraud research and modelling, and the ability for customers to tailor the platform for their specific needs. As a result, Forter is trusted by Fortune 500 companies to deliver exceptional accuracy, a smoother user experience, and elevated sales at a much lower cost. Forter was recently named the Leader in e-Commerce Fraud Prevention by Frost & Sullivan.

Forter is backed by $100M of capital from top-tier VCs including Sequoia, NEA, and Salesforce.