ECOMMERCE FRAUD TRENDS 2020

13 leading eCommerce fraud prevention solutions tell you the threats you need to prepare for in the coming year.

www.merchantfraudjournal.com

Table of Contents

Fraudsters Will Not Make It Any Easier on Merchants in 2020

Ecommerce fraud continues to rise, and fraudsters continue to innovate new ways to defraud honest merchants. This includes new strategies like synthetic identity fraud as well as new tactics like SIM card swaps. Meanwhile, technology continues to advance; it's easier and easier for thieves to perfect and scale their operations. Newcomers and wannabe hackers can easily buy personal information, credentials, and credit card numbers stolen with algorithms and sold anonymously on the dark web.

That's just the chargeback fraud problem. Sophisticated hackers go straight for merchants' bank accounts with complex account takeover fraud (ATO) attacks that target SMBs and enterprise brands alike. These attacks increase in sophistication and audacity every day, making it harder for employees to detect them. FireEye, a security platform, estimates that 7/10 phishing emails are opened by the intended recipient.

Unfortunately, many merchants and companies respond to these threats incorrectly. Merchants respond to eCommerce fraud solely by trying to prevent chargebacks — even though the amount of revenue lost by declining good orders can exceed chargeback losses. Companies respond to ATO attacks either with generic tools provided by their email provider — a strategy proven to be ineffective — or by ignoring the problem all together.

Invaluable Insights to Protect Yourself Against eCommerce Fraud

We put this guide together to help merchants, SMBs, and enterprise organizations do better to protect themselves effectively against threats. It consists of interviews with thirteen of the most well-known and respected eCommerce fraud prevention solutions available today:

Kount

DATAVISOR

SIGNIFYD

sift

clearsale

Nethone

PRECOGNITIVE

SEON

NuData Security

mastercard

FORTER

Ravelin

Fraud.net

We asked these experts a series of questions about how merchants can protect themselves. Participation was entirely free; Merchant Fraud Journal did not receive a single penny from any solution for their inclusion. We simply reached out to solutions we know are at the forefront of today's emerging fraud prevention technologies. They did not disappoint us. They answered our call with valuable insight on a number of topics, including:

- Chargeback prevention
- ATO Fraud
- Preventing False Positive Declines
- Emerging fraudster methodologies
- Machine Learning and Data Analytics
- Fraud prevention best practices

Merchant Fraud Journal's mission is to foster collaboration between fraud prevention experts, and then pass that knowledge on to merchants. We are confident that you, our community of readers, will find this guide to be a valuable resource for improving your own understanding and practice of eCommerce fraud prevention.

Sincerely,

Bradley Chalupski - Editor-in-chief

&

Dan Moshkovich - CEO

ClearSale

ClearSale is an eCommerce fraud prevention solution with nearly two decades of experience, and more than 1,000 employees servicing 3,000+ brands (including enterprise retailers like Chanel, Walmart, Sony, and Rayban) around the world.

www.clear.sale

What are the technological trends in 2020 that will help merchants deal with increasingly sophisticated fraud attacks?

I see three main trends in fraud prevention that will be coming center stage in 2020: **Ensemble Modeling, Hybrid Scoring,** and **Behavior Analytics.**

Fraud patterns have become increasingly sophisticated, and as such, fraud prevention teams have employed mathematicians, statisticians, and data scientists to find techniques that will help them predict with more accuracy and speed the behavior that results in fraudulent orders. These professional fraud investigators use a wide range of new and advanced methods like neural networks, logistic regression, deep learning, etc. that pull together different variables to understand fraud behaviors more completely. However, each methodology is unique to the person or organization that is building it. So, let's say you have three different fraud scoring procedures built by three different parties that are each being used by fraud prevention teams worldwide. But, how does a fraud team know that one singular methodology works best? Chances are, they each have different strengths and weaknesses. This is where **Ensemble Modeling** comes in. Ensemble Modeling allows you to combine the results from multiple fraud score processes to get a single score that encompasses the precision of each model employed. Ensemble Modeling will allow us as an industry to come together for the greater purpose of fighting fraud globally and allow for more innovation in the marketplace.

Fraud scoring and rules-based systems have been in place for the entire lifespan of e-commerce fraud prevention, so it seems odd that I would see this as a trend for 2020. However, I believe that Hybrid Scoring – while not new to the industry – is underused and will become a more integral method used by fraud prevention teams. The fact of the matter is that until just a few years ago, rules-based systems were used by most fraud protection teams, even though machine learning was available. Rules-based systems are clean and simple and provide a scoring that feels black and white. Businesses love this kind of scoring, but unfortunately reality is not as clean and simple as rules-based would have you believe. Machine learning can compensate for some of the more nuanced fraud behaviors that rules won't account for. In the same respect, the rules were created because they work as a foundation for assessing risk. One, without the other, gives only a segmented view of the fraud risk level, whereas together, they can work to develop a more profound view and a more accurate fraud score.

While behavior analysis isn't necessarily new to the market, and has been trending for a few years, I see it emerging as a leading technology in the coming years. As the tech for biometrics and behavior analysis is becoming more advanced and easier to implement, it is becoming a standout tool for predicting fraud. **Behavior Analytics** relies on unique behavior to build a profile of "normal user behavior" that can be used as a template to flag any behavior that is outside of the normal template. Behavior can be tracked down to biometric analysis, such as keyboard strokes and pressure, mouse/swipe dynamics and navigation habits. Since this technology is still new, I'm excited to see how fraud prevention teams manipulate and expand it. The more we use it, the more variables and dimensions we will find within it, and the opportunities are endless.

How do you see the implementation and enforcement of PSD2 impacting the way international merchants doing business in Europe will think about fraud prevention?

First off, it's important to note that I'm very concerned about the lack of knowledge about PSD2 and how it will affect this industry. Even businesses in Europe overwhelmingly either do not know about the regulations or have no plans in place to meet the deadline. I see that this will be an ongoing issue in the year to come, and I'm worried about the potential risk that merchants are facing if the regulation is ignored.

Part of the PSD2 directive is the implementation of Strong Customer Authentication (SCA), which requires a secondary security step to complete any transaction. Up until now, making online purchases might require only a debit or credit card number and security code, or -- when using a platform such as Google Pay or PayPal – a login and password. Now, buyers will need a second security factor to complete payments. For example, instead of typing just the CVV code, SCA might ask the user to enter a code generated by their banking application as a second step. This means that even if one element of an SCA transaction is compromised, the other elements will still be secure.

While most would agree that this extra step is crucial to ensure the best security standards, the directive will put a lot of stress on the customer experience. The new policies will impact the speed and convenience of online shopping, and ecommerce experts are predicting that the new regimentation will lead to increased drop-offs at checkout. Due to this obstacle in a consumer's ease of use, I foresee that businesses will be looking for ways to lower their fraud rate in order to qualify for the exempt window. While I sympathize with the businesses who see this as an obstruction and the consumers who see this as an annoyance, I am optimistic that PSD2 might help lower fraud, which in the long run, is better for all parties.

What is the biggest 2020 trend that you are preparing for that you believe people aren't talking about enough right now?

There is a big problem in the e-commerce fraud market – organized fraud attacks. The solution to it is experienced Group Analysis. I think the fraud market is too preoccupied with transactions as single entities, but I hope that in the year to come, seeing the big picture will be more commonplace in the industry.

All too often, fraud prevention teams spend an incredible amount of time and resources evaluating the risk of a single transaction, so they can easily miss that there's a fraudulent pattern happening. For example, a fraudster places an order with someone else's card. The transaction is approved because the credit card, name, address, etc. all data points match. But, through various methods (contacting seller directly to change shipping address, doing a change of shipment with shipping company, etc.) the fraudster can redirect the goods so that it never reaches the rightful owner of the card. Because this is all done after the transaction has been approved, it is very difficult to catch this fraud using the traditional methods.

Patterns like the example above are not uncommon, in fact, they are becoming more and more commonplace. Organized fraud rings made up of teams of skilled e-commerce criminals are able to pull off schemes like these on a large-scale. Even a single fraudster could easily purchase hundreds or thousands of credit card information on the dark web, and with a little ingenuity, find ways to circumvent traditional fraud protection systems to achieve a successful pattern of fraud.

So, what is the solution to this kind of fraud? **Group Analysis** is the trend that our industry needs to focus on. Taking a step back and looking at the patterns of fraud as a big picture, and not just one transaction at a time, is the only way to spot these organized fraud attacks. So, let's say in a certain region of a certain city, the average number of online orders per week is 100. Then suddenly, the order count in that zip code sees a huge burst to 300 or 400 orders. These orders look legitimate, all shipping addresses and information is a match to the rightful cardholders. But, if we can catch that the normal pattern has changed and take a closer look at these purchases, we might see that the Bank Identification Number (BIN) of all the cards is the same. This means that this bank was the recent victim of a breach and the card information was sold online.

By educating fraud prevention teams on how to spot patterns through Group Analysis, we will hopefully see the eradication of these kinds of organized fraud attacks.

Rafael Lourenco
EVP, ClearSale

Leading smart people to solve complex problems in dynamic environments is Rafael's signature skill. As ClearSale's Executive Vice President, Rafael combines the company's innovation-driven culture and emphasis on communication with a deep understanding of the statistical tools that underpin excellent fraud protection.

Rafael represents one of the world's most experienced and largest firms of its kind, with more than a decade of e-commerce fraud detection and prevention services in major international markets. From his base in Miami, he oversees ClearSale's US anti-fraud operation by leading its commercial, statistical intelligence and IT teams and providing technical and executive management for all the operation's employees, both in the US and in Brazil.

During the decade he has spent with the company, Rafael planned and executed ClearSale's international business unit, directed ClearSale's statistical intelligence area, and helped manage the company's growth from 25 to more than 700 employees, including more than 500 highly trained fraud analysts.

Covery

Covery is a global risk management platform helping online companies solve fraud and minimize risk. We focus on the universality of our product and its adaptation to any type of business, based on the individual characteristics and customer needs using both rule-based and machine learning approaches.

www.covery.ai

What are the technological trends in 2020 that will help merchants deal with increasingly sophisticated fraud attacks?

The first one that is worth mentioning is device fingerprinting technology. Today we see the constant multiplication of devices used by customers of high-risk and low-risk industries, especially in the eCommerce branch. It embrangles companies with the question of how to distinguish good customers and fraudsters. Device Fingerprinting solves this issue efficiently.

The second technology trend, which actually is not a trend but a must is enhanced due diligence that checks the source of funds coming to business from both individuals as well as other businesses. It also should be combined with strong AML software. AML and KYC are all over the gambling and iGaming industries with strict regulations.

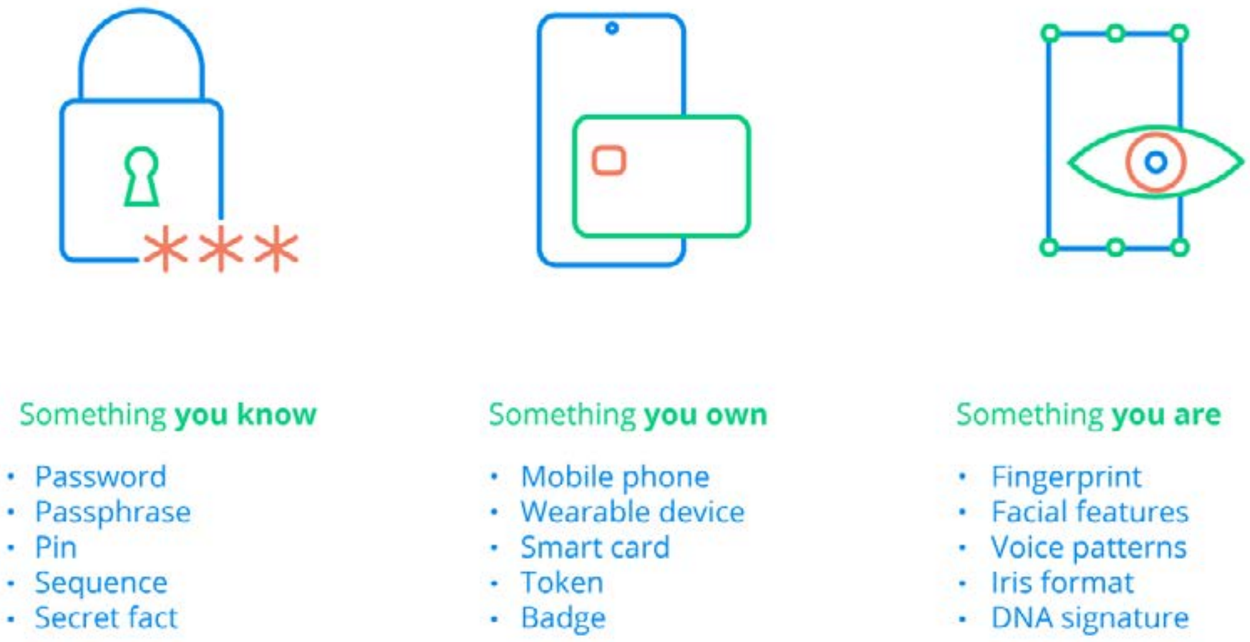
The third one and yet a must for eCommerce, gambling, and iGaming is age verification software.
No need for an explanation here.

And the last one, which is more about the approach and not about the trends, is Machine Learning, that in combination with DF helps to detect VIP customers, and sends suspicious to a check through the rule-based system.

How do you see the implementation and enforcement of PSD2 impacting the way international merchants doing business in Europe will think about fraud prevention?

Payment Service Directive 2 comes into effect in September 2019. The implementation of PSD2 will definitely help businesses across Europe to change their attitude toward fraud prevention. The main aim of this document is to establish new ways of customer protection, thus ensure transparent, safe and secure payments for businesses.

One of the most crucial components of PSD2 that will change the way how companies deal with customers is Strong Customer Authentication (SCA). Payment services and payment service providers will be obliged to put SCA to transactions. SCA is a process of customer authentication, which requires two or more pieces of information about the customer to confirm the transaction: knowledge (something customer knows), possession (something customer has), inherence (something customer is).



Despite all the complexity of SCA, there are some exemptions that will help businesses to save payments quick and easy for customers. PSD2 is a huge opportunity for businesses to change their fraud prevention perspectives and update their services and platforms, be more customer-oriented.

Indeed, it is hard to foresee the real impact of PSD2 on fraud prevention until the end of 2020.
The real outcome will appear in 2021 when all the integrations and updates inside businesses will come into effect and when they'll have full data and statistics to analyze the effect of PSD2 implementation and behavior of their customers.

What is the biggest 2020 trend that you are preparing for that you believe people aren't talking about enough right now?

The new age of FinTech definitely. 2020 will become a new era for internet bankings. We predict a great amount of new financial companies with no physical offices, with virtual cards and with features of classic B2C smartphone banking. More and more payment services develop their mobile apps to ensure instant service for their customers. However, prompt service will require prompt solutions, prompt safety for both the company and the user.

“Prompt” here stands for “automation”. 2020 will be a year of automation of all possible processes inside the payment platform, especially the automation of Enhanced Due Diligence and AML procedures. Internet banking is a buzzword today, automation - not yet. Nevertheless - automation is a king because automation saves the time of your customer, and your customer is the only one who rates you.

Pavel Gnatenko
Head of Product, Covery

Pavel has a master’s degree in intellectual systems for decision-making. He is a risk management expert with more than seven years of experience in the fintech. Currently, Pavel is focused on developing Covery - next generation of risk management platforms.

Datavisor

DataVisor is the leading fraud detection company powered by transformational AI technology. Using proprietary unsupervised machine learning algorithms, DataVisor enables organizations to proactively detect and act on fast-evolving fraud patterns, and prevent future attacks before they happen. Combining advanced analytics and an intelligence network of 4B+ global user accounts, DataVisor protects against financial and reputational damage across a variety of industries.

www.datavisor.com

What are the technological trends in 2020 that will help merchants deal with increasingly sophisticated fraud attacks?

Fundamentally, it comes down to adopting powerful, machine learning-powered fraud detection that will allow them to scale their growing digital business, while delivering a seamless customer experience.

While interlocking and independent third party products can be cobbled together to create temporary defenses against increasingly destructive and sophisticated threat actors, this is ultimately not a sustainable strategy. In 2020 we will see merchants become increasingly reliant on comprehensive fraud management solutions that combine transformational AI-powered technology with a streamlined workflow to enable proactive protection against both known and unknown threats.

Armed with AI-powered fraud detection, merchants will be empowered to create a better, more frictionless experience for good customers, while keeping fraudsters at bay and at the same time being better able to manage their appetite for risk.

How do you see the implementation and enforcement of PSD2 impacting the way international merchants doing business in Europe will think about fraud prevention?

With PSD2 enabling consumers to use third-party providers to manage their finances, it represents a new world of risk for banks.

On the consumer side, it will result in more ways to pay that are quicker and more user-friendly than before. PSD2 also brings with it more transparency regarding costs and protects banking customers from unknown charges. With this, comes less liability on the consumer side for fraudulent transactions. The theory is that this will result in new competition in the payments space that will ultimately benefit consumers with not only more choices, but a better overall experience.

For non-banks, corporates, and new FinTech innovators, the open banking provisions in PSD2 will enable them to directly access consumer bank accounts to perform payments activities and/or gain access to customer data. This represents a significant win for them in this regard.

The final beneficiaries of PDS2 are the fraudsters themselves. Having more third-party providers, more APIs, and new (and untested) product offerings, will result in additional points of access. This gives them new ways to potentially steal data and a plethora of platforms to open fake accounts to further obfuscate their activities. One can see how this open environment becomes a problematic area for banks. They will be forced to provide third parties with access to payments accounts, exposing themselves more than ever to new risks. they'll be more exposed than ever to new risks. This puts them under increased pressure to double down on things like account validation and login authentication.

The increasing number of role players in the payment ecosystem will play to the strengths of modern fraudulent practices - the ability to move quickly, adapt consistently, and operate at scale. Ultimately, PSD2 ramps up, by orders of magnitude, the perennial challenge of balancing consumer experience against risk, as it plays out in the context of growth and market pressure.

What is the biggest 2020 trend that you are preparing for that you believe people aren't talking about enough right now?

Online marketplaces have become increasingly popular for consumers worldwide. But the proliferation of fraudulent accounts has resulted in the introduction of multiple layers of authentication factors to verify the validity of a user's identity. This adds friction to the customer experience, resulting in a negative view of the service provider.

Even though multi-factor authentication increases the chances of detecting a fraudulent account, or even possible identity theft, it is extremely cumbersome for users. In some cases, authentication happens to be based on data purchased from third parties, which consumers consider to be private information.

However, there is another way. DataVisor is exploring the utopian vision of "zero factor authentication". This uses advanced technologies to build a digital DNA that integrates online behaviors (across device, activities, and biometrics) to uniquely identify each customer. With AI, the reality of this is closer than we think.

There are three critical elements to realizing this vision:

- Robust collection of more fine-grained data that will form the basis for deriving the digital DNA - an emphasis on quality rather than volume of data;
- Constant analysis of data (users are continuously "re-authenticated" passively instead of using authentication at a given point in time); and
- Transparency (users become part of the customer journey and have better control and influence over how their identity is being built and used as well as being able to opt-in or opt out of zero factor authentication).

Dr. Yinglian Xie
CEO & Co-Founder, Datavisor

Dr. Yinglian Xie has over 10 years of experience in security, specializing in fighting large-scale attacks with AI and Big Data technologies. Previously, Yinglian worked at Microsoft protecting hundreds of millions of users across a wide range of Microsoft products and completed both her PhD and post-doctoral work in Computer Science at Carnegie Mellon University.

Forter

Forter is the leading e-commerce fraud prevention company, providing mechants with an end-to-end, identity-based solution that offers protection during the entire customer lifecycle. Forter protects customer trust and company revenue with exceptional accuracy, in-depth knowledge of customers, increased approvals, and near elimination of false positives for more sales and happier customers.

www.forter.com

What are the technological trends in 2020 that will help merchants deal with increasingly sophisticated fraud attacks?

Merchants are under pressure to satisfy consumer expectations for instant gratification, which means making the customer journey as smooth as possible. But, many of the same reforms to improve customer experience also hamper merchants' ability to ensure security and prevent fraud. We've seen higher rates of fraud attacks in areas where friction-free customer experience is the most highly valued, such as travel. Fraudsters are increasingly capable of exploiting the vulnerabilities exposed by the drive for seamless purchase journeys. For example, online travel agencies are struggling to combat fraudsters who set up fake webpages with their branding, pretending to be legitimate. Consumers think they are buying a holiday from a real online travel agent, but end up being duped out of their cash. This leaves the consumer unhappy and real online travel agents have to deal with the fallout of mistrust.

However, travel agencies and other online merchants can achieve both security and seamless customer journeys simultaneously. Machine learning and active modelling technologies can be used to implement identity-based verification and real-time decisioning at any point in the customer journey, so merchants can rest easy knowing potential fraud can be spotted and stopped well before a payment is made. Such a system paves the way for an overall smoother purchase process because bottle-necks created by checks at the payment stage are removed.

While technical expertise will always be the driving force behind effective fraud prevention, automated systems mitigate the inaccuracies that occur as a result of human decision-making alone, while increasing the speed of checks. It's these technologies that will enable merchants to future-proof their fraud prevention and detection systems, while improving customer experience and boosting their competitiveness.

How do you see the implementation and enforcement of PSD2 impacting the way international merchants doing business in Europe will think about fraud prevention?

The enforcement of the Second Payments Services Directive (PSD2) within the EU will lead fraudsters to target other regions where security measures are less rigorous. Multi-national merchants need to be aware that fraudsters aim to be efficient with their activity – they will find the easiest means to maximize their gains. PSD2 will in turn, drive fraudsters committing more basic fraud attacks to regions such as the US, the Middle East, and South-East Asia.

However, PSD2 does not remove the need for merchants in Europe to worry about fraud attacks. On the contrary, PSD2 concentrates specifically on security at the point of payment only, leaving other areas of the customer journey vulnerable, and more attractive as potential targets. Fraud attack methods have evolved to take advantage of this – in recent years there has been a significant rise in account takeover attacks (ATOs), where criminals can deploy login details to conduct fraudulent purchases through compromised accounts. Other kinds of attacks have also become more attractive, such as loyalty fraud, where criminals leverage merchants' customer loyalty programs to complete transactions – especially susceptible as consumers are less likely to monitor these points as closely as their bank balances.

With all of this in mind, merchants need to be aware of how fraudsters will respond to the implementation of PSD2 and act now to defend against these developments. Fraud attack methods are well ahead of regulatory changes, so basic compliance is never enough for truly effective fraud prevention.

What is the biggest 2020 trend that you are preparing for that you believe people aren't talking about enough right now?

Traditionally, fraudsters have initiated broad, indiscriminate attacks on merchants to hedge their bets. But, recently, we've seen a shift in how attacks are conducted. Instead, fraudsters are implementing more targeted and sophisticated attacks by leveraging technologies to help them bypass anti-fraud systems. To do this, a growing number of criminals are working collaboratively as 'fraud rings' to build on each others' strengths and to drive greater results. As a result, operations can be scaled quickly, enabling these criminals to exploit both merchants and consumers before fraud teams can identify and prevent attacks.

The rise in fraud attacks prior to the point of transaction is an important trend. While the industry is focused on strengthening security measures at the point of payment with PSD2, merchants are often neglecting the steps leading up to this point. Major data breaches continue to compromise vast amounts of personally identifiable information (PII), making attacks such as ATOs more common. Highlighting the importance of comprehensive anti-fraud measures that cover the entirety of the customer journey is an area that will continue to evolve.

Michael Reitblat
CEO, Forter

Michael is the co-founder and CEO of leading e-commerce fraud prevention company, Forter. Michael began his career in Israeli military intelligence, training in cybersecurity techniques and the prevention of criminal cyber activities. He played a key part in building the first company to specialise in online payment fraud, Fraud Sciences. After the business was acquired by PayPal, he helped to develop the successful fraud prevention system that the payments giant uses to this day. Michael co-founded Forter in 2013 to realise his vision of fraud-free e-commerce. Additionally, Michael works with NGOs to help develop digital payment accessibility in developing countries.

Fraud.net

Fraud.net operates a real-time fraud detection and analytics platform, helping enterprises quickly identify transactional anomalies and pinpoint fraud using big data and live-streaming visualizations. The platform allows organizations to monitor their fraud program's performance, identify process improvements, and gain insights into developing fraud trends in minutes instead of months.

www.fraud.net

What are the technological trends in 2020 that will help merchants deal with increasingly sophisticated fraud attacks?

Fraud is more nuanced, more complex and evolving faster than ever before. Perpetrators are armed with increasingly powerful computing, detailed consumer data, advanced algorithms, and more capital. These groups can successfully iterate their way to defrauding even our most revered companies, circumventing even the most advanced defenses from this past decade.

For years, it was enough for a large organization to look only inward for the data needed to build their risk management program. Some companies would share blacklists of single-dimensional metrics (names, addresses, emails and phone numbers), usually with some degree of success. Today, however, fraudsters' ability to purchase or manipulate identity elements renders both strategies relatively ineffective.

Data Enrichment

Credit agencies and identity assurance companies that can help mitigate risks of identity theft and more traditional fraud types. If industry regulators don't already require you to build a comprehensive profile on your customers, you will likely find a bank-level 'know your customer' analysis to be an invaluable tool both in containing application fraud and in growing your business. Biometric-based identity vendors are also able to address more specialized needs for identity verification. To help capture contextual variables, there are also data vendors specializing in everything from social media to the dark web, many of which should be evaluated and whose ROIs can be easily measured.

Consortium & Collaborative Data

Above all, collaborate. Fraud.net operates a modern consortium, which includes over 2,000 features and attributes to enable the hundreds of participating enterprises to identify and prevent fraud on its first attempt. We have seen and 'fingerprinted' over 600 unique fraud methods in the past year alone. For those not in a network, it would be economically infeasible to identify these on their own as it would involve being hit each type of fraud.

Platforms & Unification of Silos

Risk departments at large organizations operate by necessity in a rules-based framework. For decades, this has been the most efficient means of segmenting and managing customers and transactions. Over time, however, the logic behind these rules become outdated and then those same rules create rigidity. As rules become more numerous and rulesets become more complex, it becomes much more difficult to understand the rules' interconnectedness, to measure their effectiveness, and to make changes without creating unintended consequences.

Agility is king in the new era of fraud prevention. Platforms are where it all comes together, enabling enterprises to organize and consolidate their siloed data. Data is then appended from a myriad of 3rd party providers, and machine learning and artificial intelligence models are applied. This makes it actionable and available to improve decision-making at every level of the organization.

How do you see the implementation and enforcement of PSD2 impacting the way international merchants doing business in Europe will think about fraud prevention?

The implementation and enforcement of PSD2 represents a significant step forward in the world of payments. Consumers will benefit from more transparency and lower fees. Merchants will benefit from extra revenues and better control over the user experience. One of the more hotly debated requirements of PSD2, however, revolves around Strong Customer Authentication (SCA). Any merchant familiar with 3-D Secure, one method of authenticating users during a credit card purchase, are also familiar with the customer friction that these extra measures can cause, unintentionally resulting in the loss of legitimate sales.

While the specific SCA requirement has been delayed largely to address this issue, designed properly, a multi-factor authentication process can be initiated on confirmation of the transaction without any downside risk. It is widely agreed that multi-factor authentication does effectively reduce certain types of fraud, such as account takeover. International merchants doing business in the EU will likely warm up to the process and ultimately apply some of these best practices in other parts of the world.

What is the biggest 2020 trend that you preparing for that you believe people aren't talking about enough right now?

With these highly sophisticated tools in the hands of highly motivated and organized rings of fraudsters, we have seen dramatic increases in a few specific fraud types. By mitigating the following risks, you will be ahead in 2020.

AI-enabled Account Takeover: Most commonly, the attackers will deploy an army of bots with credentials that have been purchased on the dark web or acquired directly in a data breach. The data can be further enriched from the individual victims using a wide variety of social engineering. The sheer size of these attacks will quickly expose which merchants and financial institutions have not taken proper precautions.

Synthetic Identity Fraud: Fraudsters are able to create fabricated identities using legitimate seed data like a social security number, leaving banks and digital merchants especially vulnerable. If you don't catch synthetic identity accounts early, they can be very difficult to catch because they exhibit all the behaviors of an ideal customer. Even companies as agile as Facebook and Google were caught flat-footed and defrauded for more than $140 million this year.

Vendor and Payroll Fraud: Corporate victims of payroll, vendor and invoice fraud are almost always targeted in advance. Fraudsters study the companies' business models, supply chain, new initiatives, and contact information for the companies' personnel. Often, the attack will be preceded by a spike in spoofed emails sent to companies' human resources or payroll departments.

Insider Fraud: If cybersecurity efforts keeps fraudsters from accessing a company's data directly, they can resort to recruiting disgruntled employees or look to exploit the negligence of other personnel. Fraudsters sometimes have gained access to employees and the company's networks for years in advance without detection. Seeking financial, identity, trade secrets and other proprietary data, their motives are usually financial.

There are over 600 distinct fraud methods, each has its own characteristics and manifests with a specific set of symptoms. But, rest assured, we are focused on and prepared to detect and prevent these new threats in 2020 and beyond.

Whitney Anderson
CEO, Fraud.net

Whitney Anderson, CEO of Fraud.net, is a serial entrepreneur with over 25 years of experience in technology, digital commerce, applied AI/machine learning, and problem-solving. He is passionate about building fast-growth companies and driving game-changing value for large organizations. Former CEO of MotherNature.com - one of Inc 500|5000 fastest growing US merchants. Prior, he held executive positions at Kroll Associates and Bank of America. Whitney is a graduate of Cornell University.

Kount

Kount's award-winning AI-driven digital fraud prevention solution is used by 6,500 brands globally, helping them to reach their digital innovation goals. Kount's patented technology combines device fingerprinting, supervised and unsupervised machine learning, a robust policy and rules engine, self-service analytics, and a web-based case-management and investigation system. Kount's solutions stop fraud and increase revenue for digital businesses, acquiring banks, and payment service providers.

www.kount.com

What are the technological trends in 2020 that will help merchants deal with increasingly sophisticated fraud attacks?

Fraud trends and technological trends go hand in hand, and the 2020s will be no different. As digital fraud evolves, so does the need to protect the entire customer journey with advanced AI-driven solutions.

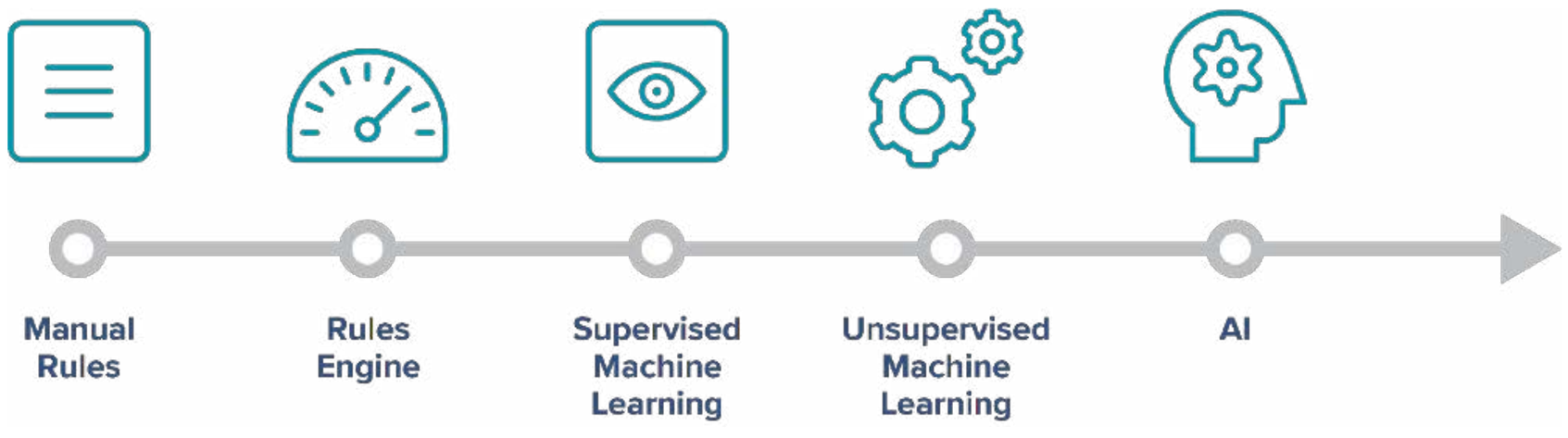
Put simply, preventing payments fraud is table stakes in the 2020s. Businesses must be, or become, mindful of every interaction between the consumer and business in digital commerce, including major vulnerabilities such as account takeover and new account creation fraud. Who is a potentially bad actor that should be introduced to strategic, additional friction? Perhaps more importantly, who is a VIP, a valuable returning customer, who should be treated to a red-carpet customer experience?

Each digital customer journey interaction is not only an opportunity to protect against digital fraud, but also to maximize relationships with customers. Only the most advanced technology can combat increasingly sophisticated fraud attacks, while also allowing the flexibility for business-driven outcomes: one trend that isn't being talked about enough right now.

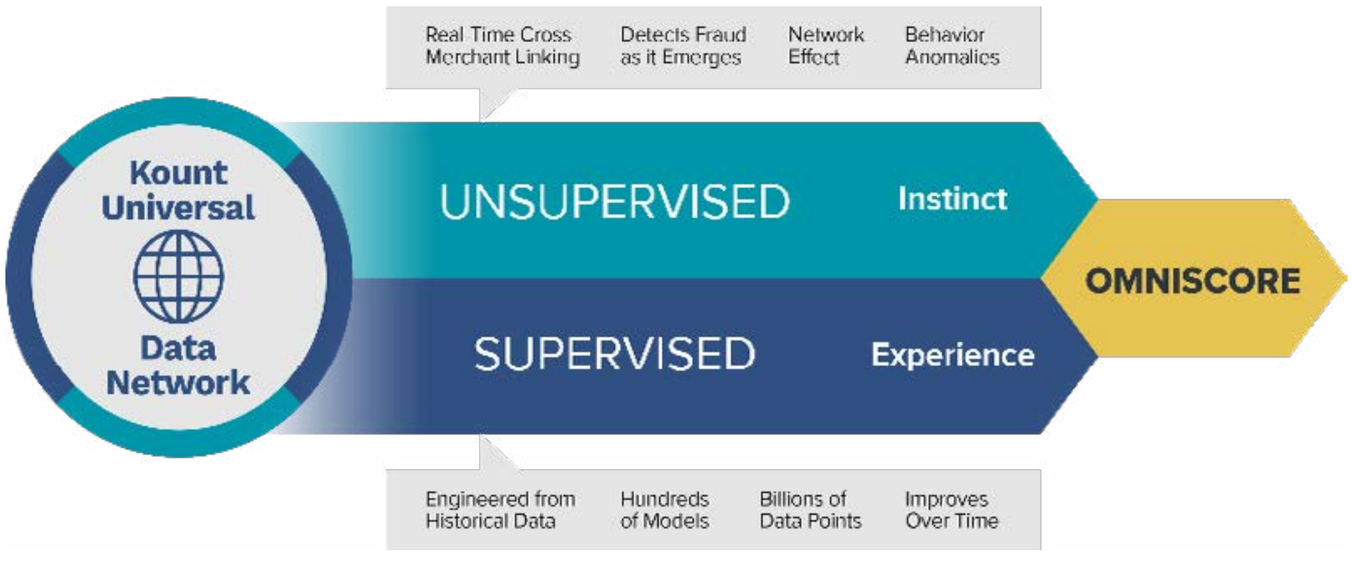
Business-driven outcomes mean that preventing payments fraud, or chargebacks, isn't the only goal. Lower manual review rates, fewer false positives and false negatives, lower operational costs, increased revenue and improved customer experiences are all desirable outcomes that black-box decisioning can't deliver. Further, certain business-driven outcomes may vary by promotion or product. A video game company that offers a high-margin product such as in-game currency would want to deliver the least amount of friction as possible to keep the player engaged in the game. A diamond company, however, may welcome a bit longer of a review process in order to avoid a costly chargeback and loss of product. And, a third company that offers a holiday weekend promotion in hopes of gaining new customers may be willing to tolerate a bit more fraud for a few days in favor of a seamless customer experience. In the next decade, consumer tolerance for friction will diminish even further, and yet, fraud will become even more complex.

To understand the future of fraud, it's useful to consider the evolution of digital commerce and fraud over the past decades. Today, consumers use mobile order and pay to buy a coffee minutes before they expect it to be ready. Shoppers use their voice assistant to place recurring orders. It almost seems absurd that we relied on the rudimentary websites, shopping carts, and payment pages of the early 2000s. Today's fraud attacks aren't conducted by a stereotypical stock image figure in a shady hoodie pounding away at keys in a basement, but rather are conducted by highly organized businesses systemically working to exploit digital commerce. Fraud rings use machine learning and bots to commit not only payments fraud, but also account takeover and new account creation fraud. The solutions used to prevent fraud must employ advanced technologies to counter evolving and emerging fraud.

Now, consider the history of digital payments fraud prevention. Before Kount pioneered the use of machine learning technology to fight payments fraud, businesses relied on manual reviews and rules engines. Then, machine learning came into play. While basic machine learning for payments fraud prevention continues to be used throughout the industry, many rely on outdated approaches that can't scale to today's attacks. Today, fraud prevention requires AI.



Supervised machine learning uses models to show the relative risk or safety of a transaction based on historic data. Effective supervised machine learning turns to a robust universal data network comprised of billions of historical transactions to present a risk score. Meanwhile, unsupervised machine learning looks for anomalies and linkages to detect emerging fraud on a faster and more scalable basis than alternatives. Kount's AI combines these two analyses with additional calculations to create a highly accurate payments risk score, Omniscore. Coupled with risk thresholds determined by the desired business outcome, Kount's AI emulates the judgment of an experienced fraud analyst.



Merchants fighting digital fraud need artificial intelligence in order to enhance the customer experience and free up the time of their fraud analysts so that they may focus on more strategic initiatives, adding new value to the business. AI allows merchants to drive business outcomes such as higher revenue, reduced fraud losses, and lower operational costs. IDC research director, Steven D'Alfonso, writes, "An optimized next-level AI fraud solution will connect to business outcomes by providing control over fraud risk thresholds, decline rates, and fraud operations costs."

Looking ahead to the 2020's, the business-driven outcomes influenced by digital fraud prevention will continue to expand. What level of friction and risk can a business tolerate at each customer interaction? As fraud evolves and new trends emerge, only the most advanced technology will protect digital innovation for the decades to come.

Brad Wiskirchen
CEO, Kount

Bradley J. Wiskirchen is the founding CEO at Kount—which is the premier fraud prevention solution for card-not present transactions. Kount protects many of the world's largest card-not-present merchants, and some of the largest acquiring banks and payment platforms. Kount is owned by CVC Capital Partners and Keynetics Inc.

Prior to December 2015, Wiskirchen was also CEO of Keynetics and Executive Chairman of Keynetics' other subsidiary, ClickBank. Wiskirchen joined Keynetics in 2005. Under his guidance, Keynetics became one of the Pacific Northwest's largest privately held technology companies, and ClickBank grew to be one of the world's largest online retailers of digital goods.

Nethone

Nethone is the global leader in AI-driven KYU (Know Your Users) solutions that help convert cyberthreats into well-informed, profitable decisions. From fraud prevention, through real-time adaptive customer segmentation, up to account takeover detection based on advanced behavioural biometrics, Nethone services simultaneously protect bottom lines and elevate profits of forward-looking businesses.

www.nethone.com

What are the technological trends in 2020 that will help merchants deal with increasingly sophisticated fraud attacks?

I believe advanced user “profiling” combined with Machine Learning will be at the centre of fraud prevention in 2020. The large majority of merchants today are either using legacy solutions which only take into account transactional data plus rules, or are simply using their PSP for conducting fraud prevention. Throughout 2020 I believe that an even larger piece of the market will migrate to tools solely based on ML (instead of a hybrid of rules and ML), and to those which gather data from the front-end of the website.

As fraudsters turn to sophisticated and dedicated tools which are made for stealing at scale, move away from device fingerprints for fraud prevention will be inevitable. Already today, we see tools selling fingerprints which have been flagged as positive by the biggest names in the industry, in order to have free reign on websites. As a result, there is going to be a much stronger focus on behavioural analytics, from voice to typing habits which will be essential for fraud prevention solutions.

All of these trends go hand in hand since it’s not possible to analyse behavioural data and thousands of data points from the front-end of websites without using Machine Learning. This is why I believe that the big winners of 2020 will be solutions with a solid background in ML and data acquisition.

How do you see the implementation and enforcement of PSD2 impacting the way international merchants doing business in Europe will think about fraud prevention?

I think that PSD2 and SCA in particular, are going to put conversion rates at the centre of all initiatives in 2020. Merchants are going to start to pay very close attention to their conversion rates as they push their liability to issuing banks. Our guess is that these rates will fall dramatically, which will push merchants to hire compliant fraud prevention solutions to conduct SCA on the merchant’s side, instead of going through the issuer. This will allow merchants to keep control of their rates instead of handing the keys to a black box.

After many years in this business, I have seen that since the risk of payment fraud cannot be eliminated, it can only be moved. The further this risk is moved away from merchants, the less efficient the system becomes in general. Each merchant's appetite for risk is different, and they should have control over what risks they want to take. We still don't know how SCA is going to be enforced by the European Banking Commission, but I believe that whatever mechanic it is, the smartest merchants will keep risk as close to home as possible.

What is the biggest 2020 trend that you preparing for that you believe people aren't talking about enough right now?

There are three areas that I believe are going to be huge in 2020, and people are simply not paying attention to as of today:

1. Call centre transactions - this channel is essential for many merchants and typically has 10 times more fraud than other channels.
2. Loyalty programs - the financial system is highly regulated, which means that money is very well protected by governments. Credits, points, and other forms of merchant-specific value are not regulated, which means that security is typically less stringent. I already see a lot of fraudsters moving to this area.
3. Topline growth - in order to prevent fraud effectively, advanced tools gather a lot of data about users straight from the front-end. This data should not only be used for fraud prevention. It's proved to be efficient in user segmentation, which applied properly, results in increased conversion and upsell rate.

I believe that these areas are not being talked about since a big piece of the fraud prevention industry has slowed down innovation. I am confident that a new wave of fraud prevention solutions is going to take over the market over 2020 using areas such as these three to beat out slower and less innovative players.

Rodrigo Camacho
Chief Commercial Officer, Nethone

Strategy-oriented professional, consultant and facilitator with broad experience in the launch of new products and brand management in international markets. With a highly diverse background, Rodrigo has a keen ability to adapt the offer of a product to different cultures. Prior to joining Nethone, he did both product and brand management in FMCG market. At Nethone, he is in charge of developing the commercial strategy as well as identifying and seizing business opportunities to sustain Nethone's rapid growth.

NuData Security

NuData Security is a Mastercard company. It helps businesses identify users based on their online interactions and stops all forms of automated fraud. By analyzing billions of events annually, NuData harnesses the power of behavioral and biometric analysis, enabling its clients to identify the human behind the device accurately. This allows clients to verify users before a critical decision, block account takeover, stop automated attacks, and reduce customer insult. NuData's solutions are used by some of the biggest brands in the world to prevent fraud while offering a great customer experience.

www.nudatasecurity.com

What are the technological trends in 2020 that will help merchants deal with increasingly sophisticated fraud attacks?

We are living in an era of sophisticated fraud. It is not breaking news that mass-scale attacks use scripts, but the interest lies in how these attacks learn. They learn from how bot-detection tools mitigate them and then build a script that bypasses those tools. Like a flu virus that evolves to survive against antibiotics, mass-scale attacks are exposed to bot-detection tools to such a degree that bad actors learn their weaknesses and adapt the scripts accordingly.

Across our clients, we see that about half of the attacks are sophisticated. An attack is sophisticated when it shows traits that require additional time and skill to prepare. For example, basic attacks spoof IP and location to fool some tools, but they don't worry about whether those IP and locations match. A sophisticated attack undertakes the extra work to ensure the fake IP and locations match and even script fake typing pauses to mimic human patterns.

Most of the attacks happen at login, where sophisticated threats can be ten times more efficient than basic attacks. Account takeover is, unfortunately, a well-established problem. Based on our network, 65% of a company's accounts are targeted at least once every month. As this type of attack becomes stronger, companies will continue to veer away from relying on bot-detection tools and will use additional security that can evaluate the user behavior such as passive biometrics.

The new-user threat:

Winning new customers is a key focus for many companies. However, new account fraud and identity theft have grown to a point where companies have to rethink their onboarding security. According to Javelin's report, The Evolution of New Account Fraud (2019), new account fraud affected 3.2 million consumers in 2018 and generated losses of $3.4 billion in the U.S. This type of fraud is increasingly affecting merchants; the Javelin report also shows that attacks targeted at online accounts (i.e., Amazon) have grown by 50% from 2017 to 2018.

These new fraudulent accounts are the source of different types of fraud such as rewards fraud, credit card cycling, or promotional abuse.

At NuData, we saw that 19% of the new accounts in the last 12 months were fraudulent; almost one every five accounts. These accounts give bad actors a safe space to develop different schemes. You can find out more about this problem here.

These accounts often use scripts, bringing us back to the same problem we mentioned earlier: can you detect sophisticated attacks or are you left to the mercy of legacy bot-detection tools? Within our network, we see that the higher the complexity of the onboarding form the lower the number of attacks that make it to the end. This is why many bad actors are moving to human farms; paying workers to manually fill the forms and ensure they don't get caught by a CAPTCHA or other bot-mitigation tool.

Technologies to fend off fraud

Authentication is tying bonds with biometrics as a reliable pairing to protect against account-related fraud. Passive biometrics is removing the reliance on credentials, and instead, adds security with visibility beyond the credentials – which can be stolen.

Similarly, the new protocol, EMV 3DS (aka 3DS 2.0), also helps merchants reduce fraud that makes it to the checkout and reduce false declines. We'll see how this new protocol will expand across regions, especially in Europe; where PSD2 is making strong customer authentication mandatory for most of the purchases in the Schengen area. The protocol has been rebuilt to aid authentication decisions and enable additional user-friendly authentication steps such as fingerprint scan.

Since fraud continues to evolve, what will be the next big thing?

Let's keep in mind that the fraud business is still a business, and the more time and effort a bad actor spends on an attack, the smaller the return will be. Like any big corporation, the margins are crucial, and if a merchant's accounts are too hard to attack they will target an alternative one. The key is to make it harder for them. We have seen bad actors go from mass-automation to human farms: the more we can do to force them to scale down and increase their costs, the more we will disrupt their business model.

Passive biometrics and behavioral analytics are proving to be successful in mitigating sophisticated attacks and human attacks such as human farms. At the end of the day, what makes a user unique is their behavior and observing these patterns behind the credentials companies can bock attacks before it's too late.

Technologies that look at how someone behaves will become, not just more commonplace, but imperative to provide lower friction on good users and mitigate sophisticated and human attacks.

Rosemary O'Neill
Director of Customer Delivery, NuData Security

A director of customer delivery at NuData Security, Rosemary delivers cutting-edge security products and services for customers across the globe. With a broad of experience that combines business expertise and cybersecurity knowledge she easily navigates the client's challenges around authentication and customer trust to provide tailored solutions. At NuData she delivers security solutions that monitor and detect fraud and unusual behaviour across a user's entire interaction on a website, from initial registration to subsequent logins, account changes, transactions, and account maintenance.

Precognitive

Precognitive is a cutting-edge fraud prevention platform that is changing the way companies fight fraud and keep their data secure. Our multi-dimensional solution combines device intelligence, advanced behavioral analytics, and machine learning to provide fraud protection services to a wide variety of key industries including banking, fintech, travel, entertainment and retail e-commerce. We offer multi-factor authentication to outmaneuver and outpace fraudsters, beating them at their own game through constant innovation. Precognitive's services are not only advanced and innovative, but we make the deployment of the technology and customer experience seamless and easy for all of our clients.

www.precognitive.com

What are the technological trends in 2020 that will help merchants deal with increasingly sophisticated fraud attacks?

Zac Rosenbauer: Behavioral analytics and biometrics are proving to be valuable solutions for merchants as they navigate sophisticated fraud attacks. While organizations continue to invest in behavioral technologies, we are only beginning to scratch the surface of what these tools can do in the card-not-present (CNP) fraud space. As attacks become more sophisticated, it is increasingly difficult for legacy systems to differentiate between fraudsters and good users. In fact, we've ran into quite a few professional fraud rings that are leveraging hacked accounts, phishing, social engineering and other methods to circumvent traditional fraud prevention systems. With this level of sophistication, traditional fraud solutions can have a hard time detecting fraudulent activity as most of the data points signify a typical consumer. That said, sometimes the behavioral data is the only factor that allows us to identify a bad actor.

Moving forward, merchants should look to incorporate new technologies that create frictionless barriers and make it extremely difficult for fraudsters to operate while improving order acceptance rates. Behavioral analytics are underleveraged by big retailers. For example, if a user has visited the website twenty times over the last six months and then overnights a $2,000 purse, we would expect this to be a user that was planning on buying the purse. Many traditional systems would flag this as fraud and either flat out reject the order or force an analyst to review the order. In order to continue evolving with fraudsters as well as their customers' shopping behaviors, retailers need to continue to invest in behavior analytics and biometrics to decrease fraud and increase approval rates.

How do you see the implementation and enforcement of PSD2 impacting the way international merchants doing business in Europe will think about fraud prevention?

Sam Bouso: Strong Customer Authentication (SCA) is the primary challenge merchants will face with PSD2 enforcement. Merchants will ultimately enjoy lower fraud rates once the adoption is complete. However, SCA presents a unique challenge for merchants as many existing solutions have shown to impact user experience and conversion rates.

As a result, savvy merchants will be looking for technology partners that can provide innovative and holistic approaches to solving SCA. They will look to those partners to provide end-to-end payment, SCA and fraud prevention solutions that seamlessly work together while still giving the merchant choice over payment provider and processing rates.

Since PSD2 forces fraud prevention and authentication into the payment flow it will also remove the need for outdated fraud prevention solutions and allows merchants to look at single product solutions like those offered by ShopRunner and Precognitive.

What is the biggest 2020 trend that you are preparing for that you believe people aren't talking about enough right now?

Zac Rosenbauer- People aren't talking enough about passwords. For the most part, software professionals have been handling authentication the same way since 1995. As we're all familiar with the current paradigm, each user has a username and password combination. Since the majority of users use the same password across multiple sites 1, getting one combination can give you the proverbial keys to the kingdom for these users.

This allows fraudsters to use good accounts to commit card-not-present (CNP) fraud and it's extremely difficult for merchants and other fraud systems to delineate between an account takeover and a good user at the time of a transaction. Many professionals implement multi-factor authorization (MFA) or other additional steps but this creates user friction. Risk-based authentication and authentication hardening are two ways to mitigate risk while improving your user's experience.

Account takeover prevention products need to be able to handle both, which can be done by leveraging a combination of behavioral analytics, behavior biometrics and device intelligence. In turn, this allows these products to make risk-based decisions and harden existing authentication systems. In addition, CNP fraud products should allow merchants the ability to see the entire user journey. Combining an advanced CNP fraud product with an updated account takeover product gives our retailers full coverage of a user's behavior from logging in to checking out.

Citations:
(2018, June 22). 52% of users reuse their passwords for different services.
Retrieved from https://www.pandasecurity.com/mediacenter/security/password-reuse/

Sam Bouso
Founder, Precognitive

Sam Bouso founded Precognitive in 2016, marking a dramatic leap forward in the way companies combat online fraud, protect consumer accounts, and authenticate users. Prior to starting Precognitive, Sam joined the product team at 41st Parameter where he enhanced their fraud technology and helped develop the 41st Parameters advertising division, AdTruth. He led global product innovation and liaised between clients, business development, and engineering to develop ad-tech and device fingerprinting products. 41st Parameter and AdTruth we acquired by Experian in 2013; Sam remained with the company to help further develop and innovate the ad-tech platform before striking out on his own to begin work on Precognitive.

Zac Rosenbauer
VP Engineering & IT, Precocnitive

Zac Rosenbauer is VP of Engineering & Information Technology at Precognitive, an enterprise fraud-prevention solution. As head of technology, Zac spearheaded many of Precognitive's growth initiatives, including ShopRunner's acquisition of the company earlier this year. After spending nearly a decade working for and with technology-focused businesses, Zac understands that successful eCommerce companies have strong cybersecurity systems and possess the ability to ingest and analyze large quantities of data. He helps businesses develop strategies for strengthening their cybersecurity posture and improving their ability to understand big data. Prior to joining Precognitive, Zac founded PointStart and was a founding engineer at Neighborhoods.com. Zac holds two degrees from the University of Toledo in E-Commerce & Information Systems.

Ravelin

Ravelin provides sophisticated technology and dedicated support to help digital businesses prevent evolving fraud threats and accept payments with confidence.

www.ravelin.com

What are the technological trends in 2020 that will help merchants deal with increasingly sophisticated fraud attacks?

There are four technological trends that I expect to see develop in 2020:

1. Increased use of data and machine-learning solutions

On the merchant side, I predict a continuation of the move from rules to data-led fraud detection methods. Today, many merchants are still using rules for fraud detection. I expect more and more will move to data-led methods using machine learning.

I also predict that we will see increased use of consortium data pools, pulling more data in house and larger companies (payment service providers) using chargeback data more efficiently. The increased use of machine learning will also help deal with these larger data sets.

2. More innovation in authentication eg. behavioral monitoring

As PSD2 takes effect across Europe and use of authentication increases, I hope that the demand for better authentication (security and experience) methods pushes providers to innovate and improve on existing methods even further. Biometrics are likely to be used more frequently for authentication methods, as we see with Apple Pay and Google Pay today.

We've also seen behavioral patterns emerge as a form of authentication. This helps determine any behavior which appears abnormal for the user such as devices used, delivery address, payment method or their current IP address when ordering. This will be especially useful to detect account takeover - when a fraudster uses stolen credentials to break into genuine customer accounts and commit fraud.

As well as account takeover, we expect to see marketplace businesses using behavioral monitoring to alert to signs of supplier-side fraud. This could be useful for businesses who connect suppliers and consumers such as taxi services or food delivery. Companies will be looking for ways to monitor behavior between suppliers and customers, for example the frequency of individuals connecting and number of cancelled orders by supplier.

3. Larger payment service providers and banks moving to the cloud

Moving to the cloud will help larger businesses to catch up with the latest fraud-fighting technologies faster. Despite security concerns, the cloud has benefits for larger companies - automatic upgrades, more predictable expenses (OPEX vs CAPEX), and the ability to scale on demand.

How do you see the implementation and enforcement of PSD2 impacting the way international merchants doing business in Europe will think about fraud prevention?

There's a chance that some international merchants may see additional fraud prevention measures as an additional expense adding to the costs of operating in the region. Additionally, as each country has its own laws on top of the Europe-wide directives, which means there are more challenges to overcome.

However, most won't want to miss out on the European market, and so we think most large international businesses will embrace the new measures. To verify this, we can look to a recent example of a Europe-wide policy - GDPR. Did this result in international merchants pulling out of Europe? No, they largely complied with it - as they are doing with PSD2. The major concern right now is not enough international companies actually being aware that the new directive exists.

In the future, international merchants may be encouraged to adopt the same fraud security measures across their business, where feasible. We can already see other countries and regions following suit and developing their own mandates, such as Australia. Eventually, it may even make Europe a safer market to expand into as fraud decreases, especially the more 'historically fraudy regions', such as the UK and France.

We've just released the Global Online Payment Regulation Report which includes regulation, top payment methods and popular payment method providers for each country in the EEA, as well as country-level 3D Secure statistics and major global regulations - see this here https://www.ravelin.com/ceros/global-payment-regulation-map.

What is the biggest 2020 trend that you are preparing for that you believe people aren't talking about enough right now?

Open Banking and increased data sharing. There are significant risks here around the fact that it will become easier for malicious actors to get hold of data and that when they do they will have more access and more opportunities for fraud.

More broadly, there is a continuing trend of fraudsters operating internationally, but many countries continue to face inwards. Without getting too political, I would like to see more cross-border cooperation to find and fight those accessing the funds and data of individuals around the globe, rather than countries focusing less on international cooperation.

Catherine Jones
Product Manager, Ravelin

Catherine Jones is the Product Manager for Ravelin Accept, a smart routing system which combines risk scoring, issuer intelligence and authentication to route payments to the path of least friction. Before joining Ravelin, Catherine had over eight years' experience in ecommerce fraud prevention, working in risk and fraud teams at Worldpay and Groupon.

SEON

At SEON, we strive to help online businesses reduce the costs, time, and challenges faced due to fraud. With a real-time, flexible API, we collect all the relevant risk-related data points, and after connecting them, we provide a risk score that leverages data enrichment and machine learning.

www.seon.io

What are the technological trends in 2020 that will help merchants deal with increasingly sophisticated fraud attacks?

The positive trend is that companies have access to larger amounts of customer data than ever before. Because “data is the new oil”, it is in their interest to gather as much of it as possible. It’s also a boost for fraud prevention, since more data points increases fraud managers’ ability to spot suspicious activity.

However, data collection takes time, and users are becoming more cautious about giving away more than what is necessary.

Our prediction is that fraud prevention solutions will increasingly turn to data enrichment to fill in the gaps. That means cross-checking information across a number of third party sources, from public blacklists to social media accounts or even known leaks. It will become faster, more efficient, and better at creating a full picture of the users without compromising the user journey.

Machine learning has also been on many fraud prevention teams’ agenda for the past few years, but we do not believe the technology will be ready to operate independently any time soon. In fact, human supervision is likely to remain a key element in fighting fraud, but more in training the algorithms rather than manually going through all the rules.

How do you see the implementation and enforcement of PSD2 impacting the way international merchants doing business in Europe will think about fraud prevention?

PSD2 is a great initiative, but if merchants do not employ proper fraud prevention solutions, it will result in high friction for all customers. This will result in more abandoned carts, higher churn at checkout, which could disrupt competitiveness.

Those who act quickly and efficiently, coming up with user-friendly solutions will have a great opportunity to acquire new customers. Those who are slow to react or who underestimate the drastic change that PSD2 is creating will be left behind - or with very dissatisfied customers.

Like GDPR, it's another customer-centric policy from the EU. But we can expect a bit of chaos and lower levels of customer satisfaction while merchants adapts to its implementation.

What is the biggest 2020 trend that you are preparing for that you believe people aren't talking about enough right now?

For us, it is account takeover. It might not seem completely new, as ATOs has seen a tremendous rise in the past few years, but it is still not taken seriously enough by merchants - and even some fraud prevention teams.

As more and more of our lives moves online, our accounts have a higher importance than ever. And because every app, service or website we log into is using different security measures, users are

Bence Jendruszak
Co-founder and Business Operations Manager, SEON

Bence Jendruszak is the Co-founder and Business Operations Manager of SEON. His vision is to create a safer environment for online high risk merchants. This is why together with his team has developed SEON, a unified risk management solution able to serve the needs of fraud managers.

Sift

Sift is the leader in Digital Trust & Safety, empowering companies of all sizes to unlock revenue without risk. Sift prevents fraud with industry-leading technology and expertise, an unrivaled global data network, and a commitment to building long-term partnerships with our customers. Twitter, Airbnb, and Twilio rely on Sift to stay competitive and secure.

www.sift.com

What are the technological trends in 2020 that will help merchants deal with increasingly sophisticated fraud attacks?

Increasing accessibility to machine learning will continue to be a major trend in 2020. While companies are transitioning into automation for their fraud prevention efforts, there will be a need to extend the application of machine learning beyond solely securing fraudulent payments. When looking at recent trends, there isn't any suggestion that account takeover won't again see a tremendous increase in volume year over year. This is built on the plethora of examples of data breaches and hacks we've seen in 2019 alone. Simply put, the credentials compromised in those breaches won't have a lasting effect on the companies listed, but at any institution where these same credentials can be tested and consumers have accounts. Therein lies the benefit of purpose-built machine learning models to account for account takeover behaviors: the scale and speed at which these attacks are happening require an equivalent technological response.

How do you see the implementation and enforcement of PSD2 impacting the way international merchants doing business in Europe will think about fraud prevention?

What's interesting is the increasing number of countries that say they will delay the enforcement of the directive. So, unfortunately for all involved, I don't think it will be as clear to the market as it would have been with a universal enforcement date in 2019.

That being said, fraud controls will unequivocally be front and center to consumers within the EEA. As such, international merchants will have to take notice, and deploy experiences that satisfy the directive yet aren't overly burdensome. The subsequent soul searching will be to determine whether you apply these standards to your entire portfolio, and not just the EEA for consistency and security's sakes. In this respect, I think there are direct parallels to GDPR. Whilst the regulation is an EU law, mirrored legislation like the CCPA eventually made its way to other markets. I have every expectation that the same will be true for PSD2 and SCA as it's tough for regulators to not advocate for legislation that is in the public interest of securing online payments.

Merchants will need to consider the creation of educational materials as well. While we have seen some countries delivering materials in market, consumers are still predominantly unaware of what's about to happen. Expressing why the changes are happening and the intent behind it will be critical to quelling presumed consumer dissatisfaction.

What is the biggest 2020 trend that you are preparing for that you believe people aren't talking about enough right now?

Card not present (CNP) fraud is still a fraction of what it will become. Given the maturity of vendors and solutions for credit card fraud, there is some belief that is a solved and/or solvable problem. However, increases in CNP fraud is a particularly scary proposition as many estimates already have this annual figure in the tens of billions of dollars. In a world where internet and mobile phone adoption rates are starting to decline year over year, eCommerce's share of overall retail remains well below a majority. As that number increases to reflect internet and mobile phone penetration, we should expect to see a rise in CNP numbers as well.

This is a large reason why accessibility to more scalable and technologically savvy solutions like machine learning is required. As companies go through their lifecycles and investment in technology, fraud will become of paramount importance.

Jeff Sakasegawa
Trust and Safety Architect, Sift

Jeff Sakasegawa is a Trust and Safety Architect with Sift. He has over ten years in the fraud prevention space, working at companies like Google, Facebook, and Square. This has afforded him the opportunity to work on many matters such as physical eCommerce, virtual payments, ad fraud, account takeovers, P2P money transfers, compliance, and more. He is now at Sift, helping to democratize access to world class machine learning infrastructure and talent.

Signifyd

Signifyd empowers fearless commerce by providing an end-to-end commerce protection platform that protects merchants from fraud, consumer abuse and revenue loss caused by friction in the buying experience.

www.www.signifyd.com

What are the technological trends in 2020 that will help merchants deal with increasingly sophisticated fraud attacks?

The easy prediction for fraud in 2020 is that it will continue to be a major challenge for online retailers and that fraudsters will continue to display an evil genius when it comes to finding new ways to take advantage of retailers.

That's been the story for years. Consider the dramatic rise of account takeover fraud in 2017 or the emergence of romance fraud in 2019. Technology — big data and machine learning in particular — have helped merchants keep up with evolving fraud tactics, but it's an effort that never ends.

In 2020, retailers will expand their focus to non-fraud chargebacks, those caused by so-called "friendly fraud" and consumer abuse.

Non-fraud chargebacks costs merchants about $15 billion annually, according to an analysis of Signifyd transaction data from its 10,000-plus customers, and it creates some of retailers' most fraught customer relations issues.

Friendly fraud chargebacks result, for instance, when a customer:

- says they never ordered from a merchant.
- or they never received a product that they did order.
- or that the product they did receive was not as described.
- or that they had canceled a subscription but continued to be charged for it.

In such cases, the customer's honesty is at the core of the complaint. Retailers are hesitant to dispute such cases; to do so means calling their customers cheaters. And legitimate customers don't respond well to being called criminals. A Signifyd/Survata customer experience survey found that 65.5% of consumers said they would never shop with a retailer again if that retailer accused them of dishonesty.

But letting friendly fraud slide costs merchants financially and marks them as a business that can be taken advantage of.

In 2020, more retailers will embrace a technology-driven answer: Using the same big data and machine learning systems that protect them from fraud to insulate them from consumer abuse. Smart machines can better identify disputes that are not legitimate, meaning retailers can with confidence confront those seeking to take advantage.

Signifyd, for instance, has extended its financial guarantee to item-not-received chargebacks and has harnessed its data and artificial intelligence to significantly automate the process of challenging and winning non-fraud chargebacks.

How do you see the implementation and enforcement of PSD2 impacting the way international merchants doing business in Europe will think about fraud?

The implementation of PSD2 is no doubt causing some short-term pain and confusion among European retailers. In the long-run, however, the new regulations will be seen as a very good thing by the retail industry.

PSD2 and it's requirements for strong customer authentication (SCA) will change the way retailers think about fraud by transforming it from a security problem to a customer experience opportunity.

SCA requires that online customers be authenticated through two of three elements:

- Something the customer knows (like a password).
- Something the customer has (like a mobile device).
- Something the customer is (like a fingerprint or keystroke pattern).

Europe's retail leaders are already embracing new technologies that allow them to conform to the new requirements without disrupting their customers' experience with requests for additional information.

Merchants have been worried about the new rules' effect on conversions, given their history with 3D Secure, which was seen as a conversion killer, and because of dire predictions, such as Stripe, Worldpay and Amazon projecting the new regulations would cost merchants €57 billion in year one.

But those fears were based on the state of technology at the time. We believe retailers in 2020 will turn to new solutions that pair a machine-learning-based SCA provider conducting dynamic fraud analysis for online retailers with the new 3D Secure version 2.2 infrastructure. SCA decisions will be passed down the 3D Secure rails to eliminate delays in approvals, minimize customer friction and maximize authorization rates.

This holistic approach allows for nearly instantaneous SCA review and more accurate decisions based on vast amounts of data processed across multiple retailers. The system will have the added advantage of shifting all liability from the merchant, either onto the issuing bank in the case of 3D-Secure-authorised transactions, or onto the SCA provider for any transaction that would require a step-up or be declined.

What is the biggest 2020 trend that you are preparing for that you believe people aren't talking about enough right now?

The impact of brands expanding into direct-to-consumer sales is a trend that will fundamentally change the retail landscape in 2020 and beyond. While not entirely new, the acceleration of the trend has been impressive in recent years and is approaching a tipping point.

The D-to-C movement has been inspired by rise of digitally native retailers (some of whom are direct-to-consumer plays) and by venerable brands' realization that selling directly to consumers comes with a host of advantages — and some challenges.

Consumers are less attached to stores and more attached to brands than has traditionally been the case. The omnipresence of online shopping means that consumers are more focused on the product they want than the merchant who is selling it.

For a brand, selling directly to consumers means it has full control over the customer experience it is providing. More importantly, selling through its own channel means that a brand has a direct relationship with the consumer. That means the brand itself collects the data from a customer's buying journey and better understands individual shoppers' wants and needs.

Having that data opens up marketing and merchandising possibilities around personalization, email and targeted ad campaigns.

That said, brands that go the direct-to-consumer route, face challenges, not the least being maintaining good relations with all of its distribution channels. Selling directly means brands are competing with the stores that stock their products. That can be managed by creating direct-to-consumer lines that are sold only online.

No question, dealing directly with consumers requires a new mindset. Brands need to speak consumers' language, understand their buying patterns. And new D-to-C entrants need to look at risk as they enter new markets.

We've seen fraud rings target large, known brands as they move into new markets. We helped one $20 billion international food brand that had to shut a regional website down shortly after it moved into a new geography. Without proper fraud protection, its losses were not sustainable.

It's a lesson D-to-C players are learning though, giving them the sort of knowledge brands can now incorporate into their direct-to-consumer strategies as the trend continues to take off.

Stefan Nandzik
VP of Corporate Communication, Signifyd

Stefan Nandzik is Signifyd's vice president of corporate communications. His "what if" approach to business problem-solving constantly challenges conventional wisdom and means that he is never afraid to upend the status quo to lead change.

Summary Conclusion: Insights and Best Practices for E-commerce Fraud Prevention in 2020

Things aren't going to get any easier for e-commerce merchants in 2020. But the nature of the problem continues to evolve. Fraud is increasingly complicated, and merchants need to take their own specific industry, product, and individual experiences into account when choosing the best solution for them.

However, fraud prevention experts continue to provide honest businesses with the expertise and tools they need to fight back. Here is a summary of the core insights they shared in this report that all merchants must pay attention to as we move into the new year:

Increasingly Sophisticated Fraud Patterns Will Require a Data-based Solution

Aided by technology, fraudsters continue to innovate new methodologies. New patterns emerge constantly, and merchants must be ready to continuously adapt. Here, machine learning is increasingly important.

Although there is no consensus on the utility of rules-based engines, the experts agree data-based approaches must be a part of any effective solution — including advancing computing techniques like deep learning. Data can come from a variety of areas — advanced pattern recognition, and running multiple models to compare results are two examples — but it must be taken into account. The days of "set it and forget it" rules-only systems are gone forever.

PSD2 Will Create New Opportunities and Threats

New consumer protections in Europe will create new pain points for merchants.

First on most minds will be the effect of additional friction on consumers. Protecting the customer experience will be paramount. In that sense, PSD2 actually opens up new opportunities for proactive companies to find a competitive advantage. Look for fraud prevention solutions to work hard to keep friction to a minimum.

Second, merchants must not let the new requirements lull them into a false sense of security. The directive only covers the point of sale — it incentives fraudsters to look for additional points of entry to bypass the new validation techniques. Look for account validation fraud to uptick considerably over the coming year as fraudsters adapt.

Finally, it's possible that fraudulent orders will make up a larger percentage of total order volume outside of Europe in 2020. Less sophisticated fraudsters may respond to additional protections by simply targeting other regions of the world. However, it will take a few months of data before any definitive conclusions can be drawn.

Account Takeover and Identity Theft Fraud will Be the Big Trends of 2020

Card-not-present fraud isn't going away. However, it's now just one category in a broader fraud landscape. Fraudsters see the huge potential returns from a single account takeover fraud attack — and their success rate remains stunningly high despite widespread knowledge about the problem.

SMBs will need to worry about fraudsters impersonating consumers' identity wholesale to avoid detection. 2020 is probably the year they begin to wax nostalgic about the days when all they needed to worry about was CNP fraud.

Enterprise organizations will face emerging threats, as well as increased volume of old ones. Things like email phishing attacks, key logging viruses, and hacked forms that imperceptibly siphon data away to fraudsters will grow in 2020. In addition, although the technology is in its infancy, expect fraudsters to begin to make widespread use of AI to create increasingly sophisticated scams. Banks, hospitals, and enterprise companies can be targeted in myriad ways, and all it takes is a single employee mistake to cause millions of dollars in damages.

“If everyone is moving forward together, success takes care of itself”

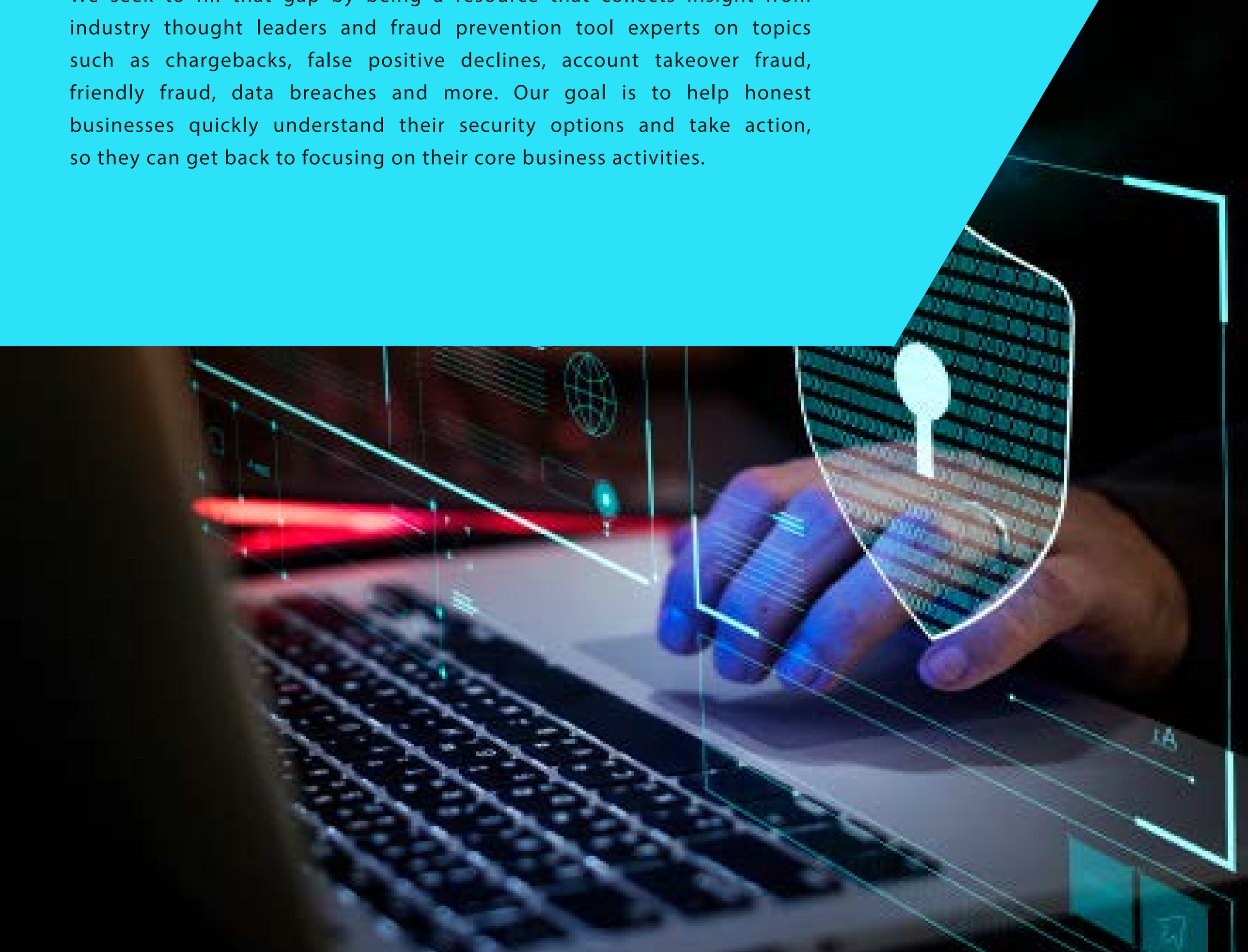
Henry Ford

About MFJ

Merchant Fraud Journal is an independent and unbiased publication dedicated to empowering online sellers to greatly reduce the impact of eCommerce fraud on their businesses. Its core mission is to break the silos surrounding merchants' internal fraud prevention processes by bringing together industry professionals to share their knowledge with one another.

Unfortunately, the business process knowledge needed for online sellers to greatly reduce the impact of eCommerce fraud is scarcely available right now. There is no single forum and resource where merchants, payment professionals, and other industry professionals could go to get educated on the myriad of challenges they face.

We seek to fill that gap by being a resource that collects insight from industry thought leaders and fraud prevention tool experts on topics such as chargebacks, false positive declines, account takeover fraud, friendly fraud, data breaches and more. Our goal is to help honest businesses quickly understand their security options and take action, so they can get back to focusing on their core business activities.



LIKE OUR REPORT? CONTACT US

Looking to create custom content, research, and reports that influence eCommerce and retail industry decision makers?

Connect with us for more details:
Dan Moshkovich,
Founder & CEO
Dan@merchantfraudjournal.com

WANT TO CONTRIBUTE? CONTACT US

Want to share editorial content and contribute to Merchant Fraud Journal?

Connect with us for more details:
Bradley Chalupski,
Founder & Editor-in-chief
Bradley@merchantfraudjournal.com

Merchant Fraud Journal

290 Caldari Road,
Concord, Ontario L4K 4J4
Canada
--

hello@merchantfraudjournal.com

www.merchantfraudjournal.com

1-(888) 225-2909