ECOMMERCE FRAUD TRENDS 2022

12 of the leading eCommerce fraud prevention and payments solutions share what you need to prepare for in the coming year.

www.merchantfraudjournal.com

TABLE OF CONTENTS

> ***2022 will be a year of huge change in the fraud prevention industry...***

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 twelve of the most well-known and respected eCommerce fraud prevention solutions available today:

ClearSale · FEATURE SPACE · OUTSMART RISK · Fraud.net · identiq · Nethone · nSure.ai · Ravelin · SEON · sift · Signifyd · stripe · vesta

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 simple 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:

- Return policy fraud
- Buy online, pick up in store fraud (BOPIS)
- Cryptocurrency fraud
- Alternative payments

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,
Merchant Fraud Journal Team

ClearSale

ClearSale is an ecommerce fraud prevention solution with nearly two decades of experience, and more than 1,500 employees servicing 5,000+ brands (including enterprise retailers like Chanel, Walmart, Sony, and Ray-ban) around the world.

www.clear.sale

How will fraudsters exploit return policies, and what will effective detection and prevention strategies look like?

We've seen 3 main ways fraudsters exploit returns:

- Wardrobing: This is the most common type of return fraud. Wardrobing is a practice where a customer will order high-end apparel and accessories, wear the item(s) with tags intact, and then return them to merchants.
- Friendly fraud: Fraudsters receive their items and then file a refund claim as "Item Not Received" (INR) or "Did Not Receive" (DNR) or file a chargeback with their credit card company.
- Return-as-a-Service (RaaS): In RaaS, professional return fraudsters work with consumers to target specific merchants and take advantage of their return policies for profit. These people are so bold, they often advertise their services online.

There are several techniques we see developing that can help curb return fraud. An easy way to start is to make sure that your return policy is clear and easy to understand at a glance. Adding tracking and delivery verification to your orders will reduce the risk of fraud claims and chargebacks. Finally, consider creating disincentives for fraud that still let good customers make returns. These can include:

- Setting time limits like 30, 60 or 90 days on returns. A good example is Amazon Prime Wardrobe, which allows shoppers free returns before the end of a seven-day try-on period to reduce wardrobing fraud.
- Making seasonal adjustments to your returns policy. For example, a clothing retailer might extend refund time limits after the holidays to accommodate gift recipients but then shorten those time limits for the rest of the year.
- Adding restocking fees on high-ticket value items. The classic example here is adding a high restocking fee to big TVs before the Super Bowl, to prevent customers from "renting" from you for the big game.
- Using hard-to-hide garment tags to prevent wardrobing.
- Requiring that customers show proof of purchase for in-store returns to prevent buy online, return in store (BORIS) fraud.
- Changing your policy to give store credit instead of refunds to discourage fraud-for-hire.

As changes are made, tracking the results to see how they impact conversions and revenue as well as fraud will help brands stay aware of what is working. By keeping an eye on return fraud and CX, you can shift the balance of fraud losses and customer experience to your favor, while keeping your good customers happy.

What are the biggest risks to the customer experience as merchants try to get a handle on the increase in pickup in store (BOPIS) fraud?

BOPIS has been an increasingly popular practice for merchants. In fact, during the pandemic, BOPIS and curbside pickup grew over 500%. Customers have really taken to the practice, especially with retailers that have been able to implement it seamlessly. Same-day delivery is impressively fast, but BOPIS offers an even faster option – customers can collect their orders as quickly as they can get to the store. Make an order and then pick it up 10 minutes later? Even Amazon can't top that.

While the CX benefits are huge, BOPIS fraud is growing and becoming an increasingly frustrating challenge for retailers. Fraudsters quickly learned that they could use stolen cards to place online orders and collect the goods within a couple of hours. Ultimately, a multilayered approach of machine learning, analytics, artificial intelligence and human strategies is required to address this fraud while also staying compliant with regulations.

However, as merchants look for the right solutions to help them mitigate this fraud, there is risk in adding friction to the customer journey. Any friction will cause a dropoff of consumers, in a recent multi-national survey of e-commerce shoppers, ClearSale found that 35% of consumers would abandon a purchase if a checkout process was "too long or complicated".

Merchants have to be hyper-aware of what friction they are adding in order to ensure legitimacy of their orders, and weigh that against the cost of falling victim to BOPIS fraud.

What fraud risks will cryptocurrencies and alternative payments create for merchants, and how should they adapt to mitigate them?"

Nearly *42% of global transactions* are made using alternative payment methods and that number is expected to increase. Ecommerce is projected to *account for 95% of purchases* by 2040 and if trends continue, most of those transactions will take place on mobile devices. Merchants who don't accept alternative payment methods will not only fall behind; they may not be able to compete at all.

Digital wallets are built with security features to protect users' data, but like any online account, these wallets are susceptible to account takeover fraud (ATO) if someone steals or cracks their login credentials. ATO has been on the rise since the start of the pandemic, and digital wallets are often a target. On top of that, merchants are increasingly reporting that it's harder to successfully fight digital wallet disputes than credit card chargebacks. One survey found that *5% of merchants reported the most success winning Google Pay and Apple Pay disputes*, while 48% reported that they were most likely to succeed when contesting credit card chargebacks.

Marchants can implement a few different strategies to mitigate these risks, such as:

- **Make sure your store follows best practices for seller protection** for every digital wallet you offer. This may require you to document every transaction from checkout to delivery. Meeting these requirements is your best bet to ensure your protection when contesting a chargeback.

- **Know which transactions are protected for different programs.** Don't conduct transactions for high-risk items through platforms that don't protect them.

- **Screen every order for fraud**, even orders from repeat customers or those who have accounts. This can weed out orders from account takeover fraudsters, and it helps your fraud algorithm learn how your good customers behave. Follow screening with manual review of each suspicious order to avoid blocking good orders along with fraudulent ones.

- **Make sure you communicate clearly with customers.** The merchant of record name on the card statement should match your website or store name, so they recognize the transaction. Track every shipment and delivery. This creates a better customer experience for them—and a digital trail for you.

What will be the biggest 2022 ecommerce fraud trend that is currently being overlooked?

Synthetic Identity Fraud is currently *the fastest-growing form of financial crime in the US* and while we're starting to see more about this type of fraud come to light, it has been around since pre-pandemic and the industry has been struggling to catch up.

SID fraud causes a number of problems for merchants—they lose goods plus processing and shipping costs, and the fraudsters also sometimes file chargebacks. In cases where merchants have extended lines of credit to these synthetic customers, they may waste money trying to recover revenue from shoppers who don't exist.

Because SID fraudsters target banks and credit card issuers first, financial institutions must use more third-party data to vet new customers. By checking to see if applicants are using data like email addresses, Social Security numbers and employers that correlate to other people, banks have a better chance of spotting fraudsters before they open accounts.

Rafael Lourenco
EVP & Partner, ClearSale

As Partner and Executive Vice President of ClearSale, 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 two decades providing ecommerce fraud detection and prevention services in major international markets. From his base in Miami, he oversees ClearSale's international anti-fraud operations 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.

Featurespace

FEATURE SPACE
OUTSMART RISK

Featurespace.com

How will fraudsters exploit return policies, and what will effective detection and prevention strategies look like?

Fraudsters know the effect the pandemic has had on merchants and as the number of online orders has massively increased (*more than two billion people purchased goods or services online in 2020*), so have the number of individuals looking to take advantage of disparate and overwhelmed workforces. It's easier to hide a needle in a haystack if that haystack is massive and you only have a few people to help find it. Volume is the key here.

Fraud prevention is not the exclusive domain of your fraud team; it needs to be at the forefront of your whole enterprise because its effects will work their way across all your teams.

Ask yourself, "does my returns team, warehouse team and fraud team share intelligence on what they are seeing, or do they work in silo?" If the returns team doesn't communicate with the fraud team on which customers have a high return rate and the warehouse team doesn't let the returns team know that a customer is returning fake goods, then you aren't going to fall behind in the fight against fraud.

What are the biggest risks to the customer experience as merchants try to get a handle on the increase in pickup in store (BOPIS) fraud?

Creating friction that drives customers to a competitor is always the biggest risk. Merchants need to ensure they have a joined-up solution, a seamless transference of data and shared processes that ensure a consumer feels secure when collecting an order, while also making the experience as simple as if they were shopping in store.

A genuine customer will ask what checks were performed when items paid for by them were picked up by somebody else, and you better have a good answer. If the instore team isn't trained on fraudsters' tactics or unable to accurately identify genuine customers so they provide a frictionless experience, then they are going to be exploited.

What fraud risks will cryptocurrencies and alternative payments create for merchants, and how should they adapt to mitigate them?

The biggest risks are not understanding the subtle differences and nuances of new payment types and treating them the same as the existing methods you utilise. This isn't a case of Sun Tzu's mantra about knowing your enemy; it's really more in line with the Spice Girls song, "2 Become 1". There's a wealth of information about cryptocurrencies, so get to know all you can and leverage some of the groups that can help navigate what is typically perceived to be a scary new frontier. It might not be the best fit for some merchants, but it cannot be discounted. Crypto is here to stay and if you aren't offering the payment types your customers want, then it's off to the pound for you. Also, it's not solely up to merchants to make sure it's done safely. Instead, this should be a collaboration with the merchant's acquirer or PSP, and fraud technology to build the most effective fraud strategy, otherwise it will pull the business in different directions and leave a gaping hole in defences.

What will be the biggest 2022 eCommerce fraud trend that is currently being overlooked?

As great as it would be to have a crystal ball and that shows the fraudsters next targets, that's not the reality. And whilst we "don't know what we don’t know", what we can do is prepare.

There are a lot of great, forward-thinking merchants that understand their vertical better than anyone, so I don't believe there is any facet of fraud that is being overlooked. What is important is being prepared to adapt quickly to changes in techniques deployed by the criminals. In the past, we'd have days and weeks to look at trends and then deploy a rule or rules to combat it, but these days, criminals - like payments - are real-time. Utilising social media communities such as on Telegram, they are communicating live and adapting to defences in real-time looking for a way in. Merchants must do the same.

How can we do this? By using advanced machine learning that can learn human behaviour from the vast number of data points that provide a 360-degree view of each customer transaction and accurately risk decisions at the same speeds needed to fulfil orders in the real world.

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.

Fraud.net

How will fraudsters exploit return policies, and what will effective detection and prevention strategies look like?

Fraudsters will likely exploit return policies through a variety of friendly fraud methods. For instance, they may continue committing chargeback fraud, which cost US businesses $4.8 billion last year, and *forms of return fraud* such as returning stolen merchandise to recover the full price, falsifying receipts, insider abuse by employees, price switching, and wardrobing, to name a few.

Chargeback fraud can affect both financial services and businesses, as the fraudster typically requests the chargeback from their card issuer whilst keeping the merchandise, and the merchant must absorb the loss. With *80% of chargebacks likely fraudulent*, and with the retail industry losing $24 billion annually in return fraud and policy abuse, this is a massive draw on merchants' profits.

Increasingly, merchants are leveraging comprehensive AI and machine learning solutions to effectively identify and stop insider abuse, by *marrying point-of-sale, card-not-present, and employee data to quickly identify friendly fraudsters* and insider threats. Joining consortium data partnerships to benefit from shared data about known bad actors is also helping merchants combat this exploitation of return policies, as well as employing *authentication technologies like 3D Secure 2.0* to combat synthetic identity and card fraud - this allows merchants and financial institutions to share contextual data and better verify customer identities.

What are the biggest risks to the customer experience as merchants try to get a handle on the increase in pickup in store (BOPIS) fraud?

One major pain point in the customer experience is card theft or card fraud, as verifying identities is made slightly more difficult for merchants due to the lack of shipping address to verify the billing address against. Certain data points that merchants have traditionally relied on for identity verification and transaction screening have been removed from the process, leading to less fraudulent transactions being flagged, cre ating a perfect storm for fraudsters to steal card information or loyalty program credentials and pick up the merchandise in-store to either keep or resell.

While merchants could likely verify in-store pickups and check IDs and credit cards, this could cause customer friction especially if pickup areas are short-staffed - the same could be said of added verification steps online. To combat this, merchants can implement fraud prevention methods that analyze customer patterns such as site behavior, prior purchases, and other key data points to protect their businesses from BOPIS fraud without causing customer friction. AI and machine learning informed by *consortium data, or a Collective Intelligence Network* is key in this particular field, as the process becomes automated and learns as merchants approve or deny transactions flagged by particular rules in the fraud management platform.

What fraud risks will cryptocurrencies and alternative payments create for merchants, and how should they adapt to mitigate them?

An emerging alternative payment method, buy now, pay later (BNPL) offers more convenience to customers and helps merchants retain revenue they would've otherwise lost from a customer unprepared to pay full price at point-of-sale. However, *even with regulations in place* to help protect both consumers and merchants with this new payment method, it is still vulnerable to fraud.

Because merchants seek to offer a seamless experience for customers and allow application for BNPL programs at checkout, fraudsters take advantage of this to submit fraudulent BNPL applications.

With a variety of forms of BNPL, one of them being the traditional split-pay format, fraudsters can take the opportunity to incur bad debt. Other fraudsters will commit chargeback fraud to recover the first payment, which can be costly. Merchants lose around $3.48 per dollar from chargeback fees, so this can add up especially as BNPL options and subsequently BNPL fraud grows.

However, merchants can employ fraud detection at key pain points in the BNPL process. Paying attention to the application and transaction stages of the BNPL journey will provide the greatest protection against BNPL fraudsters, as these are the points with the greatest potential for fraudulent activity. A multi-layered policy works best: requirements shoppers must meet to qualify for the payment plan, updating return policies, and identity verification at the point of application and transaction can effectively mitigate BNPL fraud and lower risk to merchants and BNPL providers, and ultimately the consumer.

This process may seem daunting, but AI and collective intelligence can make this process easier - for example, *Fraud.net's Application AI* analyzes previous outcomes or known compromised identities, using billions of data points in this process to flag potentially fraudulent applications. This makes it easier for the merchants' fraud prevention team to analyze potentially risky applications without increasing customer friction.

Transaction AI, also by Fraud.net, offers security at the farther end of the BNPL journey, providing protection against fraudulent transactions. With identity verification and customer behavior analysis, this flags information associated with known compromised identities or potentially fraudulent customer behavior.

What will be the biggest 2022 eCommerce fraud trend that is currently being overlooked?

Data breaches have been *on the rise for the last few years* - in 2020, incidents increased by 273%, and while rates have slowed in 2021, these are still a major threat to merchants. The harm that merchants may face is the compromise of localized information which only harms the business, or worse - customer data, putting thousands if not millions of merchants' customer base at risk. These attacks are often also events for credit card and identity theft, credentials that will later be used or *sold on the dark web for fraud purposes*.

Vulnerabilities across merchant operations as well as within the customer journey can contribute to this is sue. With business email compromise increasing at a rate greater than 2370% since 2015, a subsequent rise in account takeover is also expected. It can have a significant impact on merchants' operating costs and lead to identity fraud and data breaches, which not only threatens customer safety but can affect the reputation of a merchant.

Email security software, especially tools powered by machine learning, can spot invoice fraud and score senders to ensure that employees don't fall victim to phishing or pharming scams. Login scoring software like *Fraud .net's Login AI* protects against account takeovers by verifying key details of the login process to prevent bots or automated logins. Merchants will be able to fight these rising fraud trends with the right toolbox, a comprehensive fraud management platform.

Kevin Shine
Vice President of Sales and Partnerships at Fraud.net

Kevin Shine is a proven leader and strategist who enjoys building sales, support, and operation teams. Kevin is responsible for revenue growth at Fraud.net, an etnerprise end-to-end fraud and risk mnagemetn platform. His management and oversight includes sales and partership teams based in the United States, England, Australia, and Columbia.

Identiq

Identiq is a peer-to-peer identity verification network that allows companies to validate new users and vouch for ones they trust - without sharing any sensitive customer data or identifiable information whatsoever.
By taking third-party data providers out of the equation, Identiq leverages the consensus of other network member companies. These include some of the world's largest consumer-facing companies, collaborating to accurately fight fraud and identify trusted users.
Recognized by Gartner™ as a Cool Vendor for Privacy in 2020, Identiq sets a new standard for end-user privacy. At the same time, it reduces false positives, increases approval rates and creates a better user experience.

Identiq.com

How will fraudsters exploit return policies, and what will effective detection and prevention strategies look like?

Fraudsters are exploiting return policies: We've heard from merchants in diverse industries that returns fraud is becoming a serious concern already, and in some cases has been for over a year.

COVID 19: The Perfect Storm for Refund Fraud

The pandemic pushed refund fraud out of the shadows and into the mainstream. It's now refund-as-a-service. Consumers, buffeted by financial uncertainty, are looking for discounts wherever they can find them - even if they need to cheat. Fraudsters are happy to oblige, for a fee.

The changes many merchants have made to their returns policies to accommodate customers during the complexities of the pandemic have worked in fraudsters' favor. Many businesses have become more flexible about delayed returns, initiating the refund process once there's proof that a package was sent. Some companies have even waived the need to return the goods at all, making the process even simpler from the fraudster perspective.

Fraudster Research Drives Refund Fraud

Fraudsters target specific merchants, diving deep into their returns policies, learning every possible vulnerability. If a merchant scans the barcodes of envelopes and enters them into their system, but also throws out any which look like spam, fraudsters exploit that. If a merchant only requires a photo of a package ready to be returned, they'll exploit that.

Beyond the level of policy, fraudsters also spend time getting to know the representatives who deal with returns for the companies they're attacking. They'll learn which representatives are responsive to flattery, or a sob story, or the threat of legal action.

In some cases, they'll learn the script off by heart, and simply feed whichever lines are necessary to make the case go their way. I've heard customer service reps say they're confident that they're talking to the same fraudster multiple times a day - but are constrained by company policy to go along with the scam, if the fraudster is saying all the right things on the call.

Detection and Prevention: Collaboration is Essential

Refund fraud has a unique challenge when it comes to detection and prevention. Since it's usually real customers who place the original order, using their real address and payment instrument, with the fraudsters only taking over to manage the refund process, this kind of fraud can be especially difficult to catch.

Detection has to involve collaboration with other departments, particularly those handling returns. Reps should be trained to recognize fraud - and able to act when they do. Data about returns fraud must be inputted into the fraud team's systems.

Education and discussion with upper management is also important. It's a policy issue as much as a detection issue; Do you have the autonomy to refuse the refund? Should you wait until the parcel has been returned - with goods intact - before refunding? Can you add a red flag to the customer's account, to prevent misuse becoming a pattern in the future?

Collaboration with other companies is also worth exploring, since once successful, the same customer is likely to attempt refund fraud against multiple companies. Sharing personal user data is of course to be avoided, but advances in Privacy Enhancing Technologies mean companies can now leverage one another's data without sharing any sensitive user information, which may be a promising avenue to mitigate this knotty problem.

What are the biggest risks to the customer experience as merchants try to get a handle on the increase in pickup in store (BOPIS) fraud?

I was privileged to host a fascinating roundtable discussion on this topic during 2021. Many fraud fighters noted that their companies were actually prioritizing customer experience over fraud when it comes to BOPIS - as long as fraud remained within acceptable levels. Where fraud spiked, ID checks were added and reduced the risk significantly, suggesting that perhaps fraudsters fear getting caught out in real life.

The consensus seemed to be that with BOPIS, as so often in fraud prevention, what's important is to view risk as a spectrum. If everything appears to check out in the online order, then friction can be avoided entirely, and the customer experience is smooth. Only if there are details which appear dubious - such as visits to the account which seem to suggest possible ATO in progress, or a sudden change to BOPIS from an address some distance away, or the choice of a store far away from the billing address - should measured friction be brought into play. The level of friction introduced, of course, should vary depending on how suspicious the activity is.

What fraud risks will cryptocurrencies and alternative payments create for merchants, and how should they adapt to mitigate them?

Cryptocurrency fraud as a payment option is almost less problematic, because there are no chargebacks. Once the money is in the merchant's wallet, there is no way to reverse the transaction. On the other hand, there are still plenty of fraudsters in the crypto realm, so your business needs to develop policies for predictable problems.
If an elderly person is tricked into buying goods on your site with cryptocurrency, what do you do? Additionally, if more merchants start accepting crypto, crypto-related fraud will likely spike, leading to higher fraud across the industry - and you need to prepare for that too.

In terms of alternative payments, you need to know who has liability. If liability is on the merchant, then that's potentially high risk, and you need to analyze and plan accordingly. You may also want to be clear on the representment requirements and dispute options to prevent spikes in friendly fraud through these payment options, where merchants might not have recourse.

What will be the biggest 2022 eCommerce fraud trend that is currently being overlooked?

There are two trends I'd look out for in 2022. First, account reactivation fraud, where a fraudster takes over a dormant account and uses it, perhaps even investing time in legitimate activity before attempting fraud. Given the amount of phishing campaigns run over the last year or so, there's a wealth of stolen account data that will be leveraged over the coming year. So login protection, and protecting your accounts more generally, not just at the point of transaction, is important this year especially.

The second trend is one I hope won't come to fruition, but I definitely see its dangerous potential. New anonymizing privacy features, like Apple's Hide My Email and iCloud Private Relay or DuckDuckGo's Email Protection beta, make it very easy for users to create burner email addresses, conceal their IP addresses, etc. If such features become popular, fraud prevention teams will suddenly be fighting with one hand tied behind their backs having to blindly trust a third party with no ability to validate user's emails, geo mismatch, or even compare to known fraud indicators on their own. All of these anonymizing features are exactly what fraudsters have been dreaming about for years - and the liability, of course, remains on merchants.

Uri Arad,
CTO at Identiq

Uri Arad, Identiq's CTO, has been fighting fraud and fraudsters for more than a decade and has seen the fraud and identity challenge from diverse perspectives: product, risk, and R&D. Before he co-founded Identiq to create the solution he'd been dreaming of for years, he was the Head of Analytics and Research at PayPal's risk department. He has tremendous experience building cross-functional teams which use the latest technological developments to create innovative products that both reduce loss and improve customer experience. Uri's expertise extends both to analyzing and meeting business needs and to an in-depth understanding of the technology that makes improvement possible.

Nethone

Nethone is a machine learning (ML) based fraud prevention SaaS company that allows online merchants and financial institutions to holistically understand their end-users—also referred to as “Know Your Users (KYU)” in industry parlance. With its proprietary online user profiling and ML technologies, Nethone is able to detect and prevent payment fraud, account take-overs with unrivalled effectiveness.

Nethone.com

How will fraudsters exploit return policies, and what will effective detection and prevention strategies look like?

The effects of pandemic lockdowns forcing retailers and shoppers online has provided fraudsters the potential to succeed with returns fraud. Many merchants have ineffective internal procedures and returns policies in place, choosing to focus on customer satisfaction and continued loyalty rather than transaction risks. Fraudsters will use stolen card details to create multiple accounts or action account takeovers (ATO) to make card-not-present (CNP) payments. They immediately return items for cash gain. This is the most common form of returns fraud, although there are many, including claiming ‘items not delivered’ and making use of receipts (reused, stolen or falsified) to process refunds.

An effective strategy is for merchants to be proactive and improve collaboration between internal departments as the problem of returns fraud is not unique to any one of them. A fraud department will have a risk-based focus, which is completely different to a customer service approach where the user experience is the most important factor when processing returns. But by working together, sharing data and introducing effective policies, returns fraud can be reduced. Measures can include tracking orders and making use of return codes to weed out suspicious users (essential in understanding the scale of the problem and how to deal with it).

Another important step is to analyse user data, looking at the entire transaction process, and not just the point when the return claim is started. There are many potential indicators of potential fraudulent intentions, most of which can be identified by analysing digital fingerprints and behavioral biometrics backed up by machine learning (ML) based models. Important indicators can be the use of multiple stolen accounts. Using the same/numerous devices to make purchases, multiple IP addresses used to cover tracks etc. Identifying suspicious patterns of behaviour such as using multiple return addresses to process refunds, frequency and number of returns and even irregular browsing history can also be invaluable fraud indicators. All the signs are there, merchants just need to have the means to identify them and act accordingly.

What are the biggest risks to the customer experience as merchants try to get a handle on the increase in pickup in-store (BOPIS) fraud?

BOPIS has skyrocketed in popularity, even more so during the pandemic. Its convenience and frictionless experience is the reason for its success, but fraudsters have taken notice too, realising they need to give merchants less details for transactions (no delivery address, chip and pin payment or signature required). Additionally, it's difficult for in-store staff to do an effective ID check. This is the case for rules-based systems which heavily rely on transaction data to make a judgement call. Once the merchant has discovered a fraudulent transaction, the fraudster is long gone with the goods and can re-sell them.

As BOPIS is a card-not-present transaction, the fraud risk falls on the retailer and its risk management vendors. But because BOPIS revenue potential is attractive, companies need to find the key to reduce fraud, which is why the answer is to use a multi-layered approach. An in-store strategy can include customers verifying purchases with their PIN (something they know) for the card used to process the transaction. Staff can also be trained to do proper ID checks. These steps can deter fraudsters.

But the risk of causing payment friction with ineffective anti-fraud systems is also real, especially online. This is why using advanced anti-fraud solutions based on machine learning is essential. A user’s device and positive/negative behaviors can be analyzed automatically in real time to identify numerous suspicious actions such as using multiple accounts, devices, IP addresses (or use of TOR), numerous failed card authorisation attempts - anything that is inconsistent with regular customer behavior. This can ensure a frictionless experience for genuine customers and weed out fraudsters.

What fraud risks will cryptocurrencies and alternative payments create for merchants, and how should they adapt to mitigate them?

Alternative payment methods are associated primarily with many unknowns - merchants lack historical transaction data and the know-how to detect new fraud patterns, while fraudsters very efficiently find new methods of circumventing existing security measures or take advantage of loopholes in regulations. There’s a general lack of readiness among merchants which is compounded by inadequate investment in appropriate fraud prevention strategies and solutions to address the risk associated with accepting alternative payment sources.

The implementation of new payment methods in the user's flow should go hand in hand with a dynamic anti-fraud tool based on machine learning. Such an approach allows merchants to quickly adapt to constant traffic and configuration changes while gaining new experiences and observations related to the specificity of alternative payment methods.

What will be the biggest 2022 eCommerce fraud trend that is currently being overlooked?

Account takeovers (ATO) have been persistent threats for a long time, but now with improving anti-fraud solutions, cybercriminals realise it's becoming harder to outsmart them. With an acute awareness that user behaviours are being scanned during eCommerce transactions, fraudsters will try to act as similarly to an original account holder as possible in a process called 'warming up the shop'. The timescales for committing fraud using this method can be quite long, and some of the actions taken by fraudsters can seem pedantic. But for the fraudulent activity to succeed, patience and acting naturally are essential.

Once ATO is complete, a fraudster will analyse the purchase history of a genuine account holder, then add/remove similar items to a checkout, sometimes buying smaller items, reading customer reviews and opinions, writing new ones. Contacting merchant customer agents to engage in conversation to build up a relationship (social engineering) is also common. The final step, sometimes days or even weeks later, is to remove unwanted items and purchase only high value items, which once received can be resold for profit. This process can go on until a merchant or original account holder discovers the suspicious transactions.

Although fraudsters try to stay ahead of anti-fraud solutions, they can slip up, as advanced machine learning models such as Nethone's, using digital fingerprinting and behavioral biometrics are continually updated and scan over 5000 pieces of data. Thanks to this, getting away with fraud is much harder.

Patrick Drexler
Head of Business Development at Nethone

Experienced sales and partner manager in the payment and financial industry with 10+ years of experience. Prior to joining Nethone, Patrick managed the partnership department at Paysafecard (for Europe and Asia), and later represented the group in Germany. For the last 5 years, Patrick has built up the partnership department at Dalenys/Natixis Payment in France and led the sales activities in the DACH area. Patrick is building and executing the business development strategy for sales and partnership teams to establish an international footprint for Nethone.

Nsure.ai

nSure.ai is an advanced fraud prevention platform. It is a solution that protects sellers of digital goods, focusing on high-risk domains, such as prepaid, gift cards, crypto and gaming. Its tailored auto-ML models collect and analyze data in real time, enabling nSure to provide payment vetting and ultimate chargeback guarantees, regardless of reason (fraud and service codes). The company reduces declines by about 70%, compared to the industry average, thus allowing retailers to recapture almost $100 billion a year in revenue lost by declining legitimate customers in these domains.

Nsure.ai

How will fraudsters exploit return policies, and what will effective detection and prevention strategies look like?

Return Abuse is a highly growing trend in our space. It's actually at an all-time high due to the covid lockdown e-commerce boom. Merchants give an inch and fraudsters and "good customers" alike are taking a mile when it comes to flexible return policies.

There are legitimate fraudsters that do take advantage of these return policies, but more so we see a rapid uptick in good legitimate customers gaming the system. This can be pretty detrimental to a merchant who is looking to differentiate with a flexible return policy. How can one protect themselves when you have supposed "good" customers also gaming the system?

In order to both protect the business and still offer a flexible return policy to your good customers; Merchants need systems in place to be able to detect and link online "entities". Meaning that a merchant should be able to determine (with a high degree of accuracy) if the same person is using multiple accounts in their ecosystem. In turn, merchants need to be able to track the reputation of this particular entity as it relates to return abuse. Do you see this entity engaging in behavior that goes against your terms of use? If so, merchants should also have the ability to dynamically restrict or loosen the policy to a particular user based on their reputation and past behavior.

Legitimate fraudsters will use similar tactics, but will highly target merchants that have both a flexible return policy and a Buy Online Pick Up in Store offering. Polices that allow customers to "buy and return anywhere" Both policies present a number of new problems for merchants. Many BOPIS policies have short pick-up windows so the ability to make an immediate decision on a transaction is particularly important. In addition to flexible return policies where a fraudster can buy online and return to any store, a gift card/credit will be especially attractive to fraudsters. Effective detection will still fundamentally come down to the accuracy of your models and their ability to evaluate risk, balance fraud mitigation, and acceptance. Making sure that a merchant with both a flexible return policy and BOPIS offering has a fraud check at every touchpoint in the consumer journey is important as well

What are the biggest risks to the customer experience as merchants try to get a handle on the increase in pickup in-store (BOPIS) fraud?

BOPIS fraud has also significantly increased due to the mere fact that fraudsters have an easier time avoiding traditional fraud prevention measures. Fraud tools have less data to go off of in a BOPIS transaction which makes it more difficult to determine whether or not the user is a good or bad actor.

At the same time, merchants that do not offer low friction BOPIS method of buying will fall way behind to its competitors that do offer this way of purchasing. In today's climate consumers love BOPIS because for many it's just an easier way for them to get the products they seek.

The biggest risk here is friction and loss of trust. Friction in the sense that a merchant needs to be able to provide a smooth and enjoyable buying experience when offering BOPIS, but they also don't want to lose trust with their good customers by letting fraudsters spoof their good customers' identities. A lot of BOPIS fraud happens when the merchant allows the buyer to allow a friend or family member to pick up the order from the store. Merchants need to have a fraud check at this point in the process to verify that the person picking up the order can be trusted.

Another big risk when offering BOPIS is that the time to make an "Approved" or "Declined" decision on a transaction is much shorter. Often times pick up windows are small and there is not much time (if any) to manually review a transaction. A merchant needs a system in place to provide instant decisions for BOPIS transactions.

What fraud risks will cryptocurrencies and alternative payments create for merchants, and how should they adapt to mitigate them?

Cryptocurrencies as a payment method definitely offer a few benefits to merchants. Merchants can process transactions much more cost-effectively and with zero risk of chargebacks. One might read that and think there is zero fraud risk to merchants. However, even though the liability of the transaction falls on the consumer, the merchant still needs to take measures to reduce consumer-related cryptocurrency fraud.

Cryptocurrencies & other forms of payment where the consumer is liable will introduce a surge of "victim assisted" fraud where the fraudster takes advantage of the good user and essentially guides them in purchasing the goods they seek on their behalf. Typically you see this form of fraud targeted toward the elderly population. It's important that a merchant is partnered with a provider that can spot and catch these trends early to help the merchant implement policies and procedures that deter this behavior.

What will be the biggest 2022 eCommerce fraud trend that is currently being overlooked?

Almost every fraud prevention system in existence today is solely set up to protect a merchant from legitimate fraudsters. Fraudsters that obtain stolen data and payment information in order to purchase and resell stolen merchant goods. Many systems today are very good at stopping fraud in this manner. But what about friendly fraud? How do you stop good customers from abusing the system without ruining the customer experience?

There is a rapid rise of Friendly Fraud (or 1st party misuse) that I believe is being overlooked. More and more consumers are understanding the ease of charging back transactions with their banks. Since liability is not on the consumer (which it should not be in most cases) then the liability has to fall somewhere. How can we (as an ecosystem) reverse this trend while still providing the ability for good customers to chargeback legitimate cases?

I think this is a growing problem that many merchants and solution providers are overlooking in 2022. It's a complex dilemma where merchants need sophisticated systems in place to not only mitigate these risks but

Miguel Mejares,
Head of Sales at nSure.ai

Miguel Mejares leads sales efforts for nSure.ai - the first platform that offers Ultimate Chargeback protection which provides merchants with 100% coverage on all chargebacks regardless of the reason (even friendly fraud). He has worked for some of the leading fraud prevention providers out in the market today. He is also a huge advocate for frictionless and fraud-free commerce. Miguel envisions a world where one day merchants no longer have to be liable for chargebacks.

Ravelin

Ravelin provides technology and support to help online businesses prevent evolving fraud threats and accept payments with confidence. Combining machine-learning and graph network visualisation, Ravelin helps businesses draw deeper insights from their customer data to detect fraud, account takeover and promotion abuse and increase payment acceptance.

Ravelin.com

How will fraudsters exploit return policies, and what will effective detection and prevention strategies look like?

92% of customers will only buy again if the returns process is easy, so generous returns policies are essential in today's competitive landscape. Unfortunately, such policies open the door to refund abuse. This type of fraud occurs when a customer uses the returns policy of a merchant to the point that it becomes unprofitable — and this problem isn't likely to slow down in 2022.

A false claim of a package not arriving is the most common form of refund abuse, while opportunists will also use tactics like faking returns, or using an item once before returning (wardrobing). What's more, sophisticated refund fraud is now an industry, with organised fake returns schemes and even the emergence of refund fraud as a service.

Refund abuse can be difficult to manage because it's almost impossible to spot at the time of purchase. Additionally, if a company starts denying customer refunds they risk losing genuine customers, or sending them down the friendly fraud route, which can result in costly chargebacks.

As such, combatting refund abuse will require careful monitoring to discourage bad behaviour, keep genuine customers, and block prolific offenders. Customer data will prove invaluable, and businesses should set a threshold for an 'acceptable' number of returns over a period of time. If a customer exceeds the limit, a warning email can be sent, or refund friction can be increased.

Graph networks are also a useful tool to spot sophisticated forms of refund abuse. Organised fraudsters may use multi-accounting techniques to request refunds on a large scale. Link analysis using a graph network helps identify connections between new accounts.

A successful strategy will also ensure fraud is not just front of mind for the fraud team. Communicating the tactics of fraudsters and implications of refund abuse to the wider business will prove vital. For example, only employees handling returns will be able to monitor red flags like parcel weight changes or packaging damage.

What are the biggest risks to the customer experience as merchants try to get a handle on the increase in pickup in store (BOPIS) fraud?

The appeal of buying online and picking up in store has grown considerably over the past couple of years, as people sought to minimise the time they spent in stores during the pandemic.

But as the appeal of buying online and collecting in store has grown, so too have concerns around BOPIS fraud, largely because of its ability to bypass basic fraud detection solutions. Fraudsters also know that retailers can be hesitant to introduce more thorough prevention measures because of the risk of harming the customer experience. BOPIS fraud attempts have increased by 7%, compared to 4.6% for other delivery channels.

If retailers begin asking for more online information, or checking IDs and verifying credit card information in store, they're taking away the frictionless experience and potentially deterring customers from using the service, or purchasing again in the future.

Additionally, if legitimate customers are turned away because of suspected fraud, it can leave a sour taste in their mouth – which won't do the brand's reputation any favours.

The best way to prevent BOPIS fraud while maintaining the optimum customer experience is by implementing a sophisticated AI-based fraud prevention solution. This way, fraud can be accurately stopped in the first instance — negating the need to add friction for genuine customers.

What fraud risks will cryptocurrencies and alternative payments create for merchants, and how should they adapt to mitigate them?

In an ever-changing payments landscape, many merchants are successfully cracking down on fraudsters using traditional payment methods. However, a worrying number still aren't investing significantly into preventing fraudulent transactions using alternative payment methods, like cryptocurrency.

Cryptocurrency has exciting potential for merchants. It virtually eliminates chargebacks, because transactions can only be refunded by the receiving party. It's also less expensive to accept than credit cards. However, it does bring about risks.

For example, cryptocurrency is highly reliant on unregulated entities, some of which will lack the necessary internal controls — leaving them more exposed to fraud and theft than regulated financial institutions. If a customer has the keys to their wallet stolen, the thief can fully impersonate them and has the same access to the money in the wallet.

To remain competitive, merchants are going to have to start looking at accepting alternative payment methods. However, they'll face the familiar problem of identifying and stopping fraud without hindering the customer experience.

What will be the biggest 2022 ecommerce fraud trend that is currently being overlooked?

One of the biggest and overlooked trends right now is promo abuse. While promo abuse isn't fraud as such, it's becoming a significant threat to businesses' profits and will continue to be a threat in 2022. This type of fraud involves customers taking advantage of offers, like sign-up bonuses, referral discounts and voucher codes. For example, customers might make multiple new email accounts to use a voucher over and over. Or, if promo codes are too simple, they can guess future codes.

This can result in eye-watering hidden costs for the business. Uber famously experienced one determined user who racked up £50,000 in future ride credits by posting a referral code on Reddit.
Ravelin's research found that more than a third (35%) of retailers saw an increase in voucher abuse in 2021. Grocery retailers saw the biggest rise, affecting 48%, with 18% noticing a significant increase. If businesses don't start to take this threat seriously in 2022, the costs will only get higher.

The true impact of promo abuse is often hard to track, so it's all too tempting for businesses to turn a blind eye. But no matter how small the discount, thousands of customers abusing the promotion at the same time can seriously erode profits. It can also damage brand identity. If a genuine customer can't redeem a voucher that's already been used fraudulently, you risk them losing trust in your brand.

Mairtin O'Riada
Chief Intelligence Officer

Mairtin is the CIO at Ravelin, which provides fraud protection for online businesses. The "I" in CIO stands for "Intelligence", and Mairtin runs the Data Science and Investigations team in Ravelin, responsible for the machine learning and graph network models at the heart of Ravelin's detection engine. He was previously the Head of Fraud at the taxi app Hailo, where he honed his fraudster frustrating skills. He is an internationally experienced intelligence analyst, with stints in Scotland Yard, the United Nations and elsewhere.

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 relevant risk-related data points. Once connected, we provide an overall risk score that leverages data enrichment and machine learning to help make the right decision.

Seon.io

How will fraudsters exploit return policies, and what will effective detection and prevention strategies look like?

A strong returns policy is vital to fortify your customer loyalty, however, once an order is placed and returned, there often isn't much a merchant can do.

Fraudsters will exploit customer-centric return policies by using stolen credit card/credentials, *double-dipping*, and bricking (the act of returning an electrical item after stripping its valuable parts, receiving both profits and refund).

For smaller merchants, losing out on both product and profit can be immensely damaging.

Thankfully, as fraud detection has become more accessible, there are numerous ways to prevent these scenarios.

First and foremost, understanding as much as possible about the purchaser helps mitigate risk immediately. Using data enrichment software such as a reverse email lookup tool can help create a holistic digital footprint analysis - all pre-transaction.

Taking a person's email address and verifying their profile across a range of online platforms can add more security in order decisions as fraudsters will not link their personal email/accounts with an abuse account.

This can also be applied to a user's mobile number; data from our social & digital profile tool has shown that a fraudulent order will often have less than two social media accounts to the email/phone number.

Return abusers who operate at scale will create multiple accounts with dud emails. By using a data enrichment tool to analyze a person's digital footprint as well as testing the domain can quickly spot potential risks.

Another strategy would be to require a customer to provide a form of identification for returns. A simple cross-referencing between the account holder and the detail submitted can show signs of potential fraud.

What are the biggest risks to the customer experience as merchants try to get a handle on the increase in pickup in store (BOPIS) fraud?

Buy Online Pickup in Store (BOPIS) has become a more convenient way of picking up goods for consumers and empowers customers throughout the entire purchasing process.

However, the circumstances can create a range of problems; from depending on the staff and their ability to spot potential fraudsters to the typical issues that come with *card-not-present* (CNP) transactions.

It is worth noting that unlike the majority of online orders that go to an address, BOPIS orders come with no delivery address. This bypasses a huge pain point for fraudsters and is a vital piece of information when authenticating a customer.

Finding the balance between risk and customer experience is always going to be a struggle but a non-optimized BOPIS process can completely damage your brand.

Merchants can consider a range of options such as enabling card authorization upon pick up but the reality is, there's no consensus on fool-proof conduct.

For example, asking a customer to bring the same photo identification as the billing ID upon pick up will work fine for the majority of people, but how are you going to allow a different person to pick it up? What if the account has been compromised?

Your fraud team needs to lean on historical data, make use of behavioral analysis and consistently develop customer profiles.

This will allow you to confidently determine that the customer has acted in a typical manner and it is them who placed the order. Communication with on-site staff is also important if a transaction has some level of risk.

What fraud risks will cryptocurrencies and alternative payments create for merchants, and how should they adapt to mitigate them?

Despite the recent hype surge, a *YouGov* survey reported that of 1,000 people across the US, Mexico, and Brazil, a staggering 98% of people don't understand 'basic crypto concepts.'

Whilst it can be tempting to add as many alternative payment methods as possible, cryptocurrencies remain unregulated and can bring anti-money laundering, counter-terrorism, and reputational risk.

Crypto transactions are also irreversible, which could make conflict situations such as item-not-received (INR) cases more delicate than they already were.

Bitcoin being decentralized does help minimize chargebacks, however, because of the volatility, the prices are not stable enough to make accepting them risk-free.

According to a survey by the National Retail Federation, US merchants lost over $25.3B to return abuse and fraudulent returns in 2020.

Businesses that accept Bitcoin must be prepared for the possibility of customers requesting refunds, meaning you will need to keep track of the initial purchased price.

Although there are a small number of people who would want to use crypto to buy goods, fiat is still dominant so merchants need to consider the risk of inviting potential money launders if you choose to accept crypto.

Customer experience is crucial for any ecommerce business and instead of avoiding alternative payments altogether, businesses need to utilize AI-powered anti-fraud solutions to identify and validate customer identities before they're able to make a purchase.

What will be the biggest 2022 eCommerce fraud trend that is currently being overlooked?

Phishing is often overlooked and even mocked by your average customer. However, fraudsters are only getting better at manipulating people and circumstances.

As the rate of online transactions increases, cybercriminals are becoming more creative in gaining access to customer data, going beyond traditional phishing.

For example, setting up fake websites and/or lucrative deals gives consumers the 'FOMO' effect and leads to hasty actions, without conducting their due diligence on the site they've clicked.

Through more advanced social engineering, fraudsters are able to extract user information, sometimes even the account itself.

Business Email Compromise (BEC) attacks are another aspect of phishing that has seen incredible growth.

According to the FBI's Internet Crime Complaint Center, BEC attacks have grown by 2370% since 2015.

Furthermore, with the growth of *deepfake technology*, fraudsters are using more creative ways to impersonate others.

Over the next decade, the need for a standard education is going to become vital to help mitigate the risks of online scams.

Tamas Kadar
Founder and CEO of SEON

Tamas Kadar is the founder and CEO of SEON. The company was founded after launching a crypto exchange and hit by staggering levels of fraud. This sparked an interest in fraud prevention. From there, Tamas and Bence (co-founder) built SEON from scratch with a mission to build an innovative, go-to solution for any online businesses affected by fraud.

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, DoorDash, and Twilio rely on Sift to stay competitive and secure.

Sift.com

What fraud risks will cryptocurrencies and alternative payments create for merchants, and how should they adapt to mitigate them?

From a financial fraud standpoint there is relatively little risk for a merchant that wants to accept alternative forms of payment. However, while cryptocurrency transactions are one way transactions that do not carry chargeback risk, the merchant will need to make the decision on how they store the currency, given the volatility of the market.

Merchants will not optimize their return on investment if their customers do not pay in cryptocurrency, but it's equally important to not dismiss the availability of crypto payments within their already-integrated payment partners.

Fraudsters are also keenly aware of the places where they can spend crypto. Once a merchant adds this payment method, fraudsters may target them as a new place to cash out illicitly-obtained coins. Despite the lack of chargeback risk, the merchant needs to prevent these purchases just as they would prevent traditional payment fraud. Why? Because a crypto fraudster does not represent good lifetime value and could prevent products from getting in the hands of a legitimate customer with a good lifetime value. What's more, a crypto fraudster may be able to identify vulnerabilities as they become more familiar with the merchant's website.

What will be the biggest 2022 eCommerce fraud trend that is currently being overlooked?

While 2021 saw the explosion of the professional refunder within FaaS (Function as a Service), I predict 2022 will bring the rise of the professional KYCer.

For example, we recently discovered that encrypted messaging apps like Telegram have become a haven for fraudsters selling identity information – both synthetic and illegally obtained – to help other would-be fraudsters bypass KYC checks to gain access to merchant services and marketplaces like crypto exchanges. Secure messaging apps keep users' identities protected and are largely unregulated, fueling KYC bypass fraud as a service.

While those eager to avoid ID checks have found workarounds to certain KYC implementations, these verification tools serve an important purpose: ensuring legitimate consumers can access the sites that they want to visit and do business on.

While ID technology can be effective, businesses should use it as part of a layered approach to prevent nefarious activity—particularly fraud. When combined with an ML-powered Digital Trust & Safety strategy, ecommerce merchants can stop bad actors both on the front end and with every transaction, all without disrupt-

How will fraudsters exploit return policies, and what will effective detection and prevention strategies look like?

Fraudsters have the time and motivation to identify vulnerabilities in merchants' return processes, and will continue to collaborate on forums like Telegram to reverse engineer, exploit and monetize refund policies.

Typically smaller, independent merchants don't have a dedicated fraud team in place, so the key is to begin planning as soon as possible. This starts with evolving beyond legacy approaches and adopting a Digital Trust & Safety strategy - one that dynamically addresses fraud while creating a more seamless experience for legitimate customers.

Effective detection and deterrence comes down to having clear return policies on the front end and machine learning on the backend to identify the clusters of bad actors that are causing the most coordinated harm. As merchants who expanded into ecommerce during the pandemic return to their brick-and-mortar operations in some capacity, they need to ensure that their online and offline systems are synced. Otherwise, they will be defrauded via items bought online and returned in store.

Traditional manual review processes and systems, such as caps on order volumes and values, aren't equipped to detect fraud during high-traffic periods. Instead, they're stopping legitimate transactions completely or creating friction within the customer journey. By implementing technologies like machine learning, retailers can better defend against fraud this holiday season at scale. Ingesting thousands of different signals beyond purchase data, machine learning systems can quickly adapt to detect suspicious activity in real-time without human intervention. This allows retailers to proactively identify and defend against fraud.

What are the biggest risks to the customer experience as merchants try to get a handle on the increase in pickup in store (BOPIS) fraud?

The biggest risk to customer experience remains customer insult rate and wait times. A customer insult occurs when a legitimate customer is unable to complete a transaction due to the purchase being mistakenly identified as fraudulent. Merchants must have a clear understanding of what their insult rate is by tracking it over time, along with the BOPIS fraud rates. If the merchant implements measures to validate the customer and the transaction to prevent fraud loss, they can't allow a line of cars to pile up waiting for their order. It's important to zero in on the problem: How do you decrease fraud while actively growing revenue? The answer is Digital Trust & Safety.

Digital Trust & Safety can empower businesses of all sizes, through the use of machine learning. Through APIs and a customizable web-based counsel, trust and safety teams of all sizes can investigate fraud patterns, automate decisions, and analyze business performance, without hindering the experience of legitimate customers.

Kevin Lee
VP of Digital Trust & Safety at Sift

Kevin Lee brings 15+ years of experience in the risk and fraud management space to his role of VP of Trust & Safety at Sift. From fake news, to payment fraud and ATO, Kevin has had to face and mitigate against various types of online abuse that have impacted billions of people. Prior to joining Sift, Kevin built and led risk, fraud and spam organizations at Facebook, Square and Google.

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.

Signifyd.com

How will fraudsters exploit return policies, and what will effective detection and prevention strategies look like?

One of the most colorful and costly ways merchants will see their return policies exploited is a variation of the old bait-and-switch. A fraudster buys a mobile phone for instance and returns a knockoff or broken model or even a box of rocks filled to approximate the weight of the latest and greatest mobile device. One bold returner even offered a *potato as a stand-in for an iPhone.*

There are less evil-genius forms of return abuse, too: Bracketing — buying several similar pieces of apparel with the intent of keeping just one and returning the rest. Or wardroving — buying a product to wear or use once or twice before returning it. Or falsely claiming a product is damaged in such a way that a return is undesirable — think reporting that a new laptop's battery is leaking.

Return scams, which the National Retail Federation says costs retailers *nearly $8 billion a year,* take advantage of merchants who are focused on providing a great customer experience. The switch scam, for instance, works because some merchants refund a return as soon as the product is on the way back. That way customers don't have to wait for their money. By doing what's right for the customer, the merchant is helping a fraudster do wrong.

No matter the form of return abuse, the best prevention is understanding the identity and intent behind every return request. Does the returner fit the profile of a serial returner? Do they fit the profile of a loyal, repeat customer?

Understanding identity and intent allows a merchant to customize its response to a return request. Should the customer receive an immediate refund? Should the merchant offer store credit? Is it the rare case in which a return should be denied?

Any merchant with any kind of sales volume, can't scale that kind of decision making. That's why successful retailers now rely on commerce networks of merchants that produce vast amounts of transaction data. That network data provides patterns that indicate whether a return is abusive or on the up-and-up. And it does so in an automated fashion, which allows return protection to scale as the business and ecommerce grow.

What are the biggest risks to the customer experience as merchants try to get a handle on the increase in pickup in store (BOPIS) fraud?

Merchants expanding buy online, pick up in store and curbside pickup have to constantly balance speed of fulfillment with protecting the enterprise. Taking days or even more than a few hours to screen orders for fraud defeats the purpose of in-store or curbside pickup.

Customers turn to in- or at-store pickup because they want their item now, or in an hour or two. If an order isn't ready for pickup when promised, especially if the customer has traveled to the store, a merchant can pretty much forget about seeing that customer again. In fact, about 53% of consumers in a Signifyd survey said they would tolerate no more than one bad online experience before deciding not to shop with a retailer again.

The solution is to determine whether the order is fraudulent or legitimate at the point of sale — as in when the customer clicks the buy button. Data-driven, machine-learning solutions can do that by relying on the signals and ultimate outcomes from millions of orders.

What fraud risks will cryptocurrencies and alternative payments create for merchants, and how should they adapt to mitigate them?

Beyond the practical challenges of accepting cryptocurrency — which currencies to accept, how to manage value fluctuations, etc. — there are particular flavors of fraud that come into play. Most of all, there is no way to know the provenance of the cryptocurrency used in a given transaction.

For one thing, the cryptocurrency used in a transaction could itself have been purchased with a stolen credit card or account information. That leaves the merchant processing a fraudster's payment and in effect contributing to the success of a criminal ring that is actively working to defraud the merchant in other ways.

Crypto-wallets can be stolen. And so, again, in such cases, the merchant is facilitating fraud.

Similarly, alternative payments such as buzzworthy buy-now-pay-later options provide their own vulnerabilities. For the most part merchants will avoid taking a loss when a BNPL order involves fraud. The firms offering the service generally accept fraud liability. But it opens merchants up to non-payment fraud and abuse. For instance, think of a customer who doesn't have the credit limit, or checking account balance (in the case of a debit card), to bracket. It takes an upfront outlay, for instance to buy three pairs of shoes or three dresses to try on and decide. With the ability to make only partial payment, that problem is solved — leading to an increase in wardrobing.

What will be the biggest 2022 eCommerce fraud trend that is currently being overlooked?

Merchants and risk intelligence professionals will need to pay more attention to the expanding the surface area of fraud attacks. With the dramatic shift to online buying during the COVID-19 pandemic fraud rings innovated, iterated and broadened their attacks to the full buying journey. While not necessarily new, attacks in the form of account takeover, policy abuse, return fraud and friendly fraud morphed and intensified.

In fact, friendly fraud, including item not received and item significantly not as described, *doubled year-over-year* in the first half of 2021, according to Signifyd data. We've seen heightened activity around account takeover and loyalty points. We saw a surge in bot attacks, both for credential stuffing, but also to facilitate unauthorized reselling.

You might recall the uproar over price-gouging among resellers of PlayStation 5s. And, of course, there was a similar *automated run on scarce graphics processing chips* in the spring and beyond.

Again, these emerging or intensifying attacks bring me back to the notion that if you know who the buyer, returner, customer is and you know why they are taking the action they are taking, you're in the best position to provide a great customer experience without having to fear putting the enterprise in jeopardy.

Stefan Nandzik
Senior Vice President, Brand Experience

Stefan Nandzik is Signifyd's Senior 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

Stripe

Stripe is a technology company that builds economic infrastructure for the internet. Businesses of every size—from new startups to public companies—use Stripe software to accept payments and manage their businesses online.

Stripe.com

How will fraudsters exploit return policies, and what will effective detection and prevention strategies look like?

Fraudsters have long exploited return policies for physical goods, but digital goods make return abuse and chargeback fraud a lot easier. Fraudsters don't have to return a physical item, and digital goods often make it harder for businesses to prove customers did receive what they ordered. We've seen increasing instances of friendly fraud on platforms selling online education courses, for example—possibly because fraudsters can copy the content before they lose access to the materials during the return and chargeback processes.

But the crux of the issue is that people want seamless buying and purchasing experiences online, including returns and refunds on partially-used digital services. That creates increased risks of fraud. And while digital merchants have implemented policies to lessen these risks—like preventing a return after an online course has been more than halfway completed, or not allowing multiple refunds to a single customer—these measures don't prevent a customer from requesting and being granted a chargeback from their issuer, for which the merchant will incur a fee.

Effective detection and prevention strategies need to incorporate both return and chargeback fraud. An effective fraud stack—especially those that pool data from large-scale machine learning engines—can identify in real time if a customer presents a chargeback risk and offer interventions to high-risk transactions, like having a customer upload an image of their card to help determine if their payment details are fraudulent.

What are the biggest risks to the customer experience as merchants try to get a handle on the increase in pickup in store (BOPIS) fraud?

A lot of the challenge with BOPIS fraud is the same as other types of card-not-present transactions: how can you build in protections to identify when credit card details are being used fraudulently—without spoiling the experience for good customers?

Adaptive machine learning isn't new in fraud protection, but its deployment at scale, analyzing hundreds of attributes for each transaction, can help make this tradeoff optimally. Machine learning has led to the creation of fraud detection tools that minimize friction for customers early on in the transaction process. In the case of BOPIS, this can translate to a more seamless in-store experience later on during pickup, saving customers the hassle of providing further identity or transaction verification in-store.

Stripe Checkout, for example, can surface captchas for ID verification when it detects suspected instances of card testing—but the power of the underlying machine learning means good customers almost never see these challenges. And as is the case with returns fraud, verifying customer payment information early on in the transaction process—in the form of 3D Secure 2 or a scanned card—can minimize the friction customers may encounter in store when picking up their items.

What will be the biggest 2022 eCommerce fraud trend that is currently being overlooked?

We're seeing that fraud is rapidly becoming a full-blown, tech-enabled professional enterprise. The increasing online availability of stolen card information, along with the proliferation of digital platforms for easily selling digital assets, mean fraudsters can make more money more easily, using automated processes to scrape the dark web for stolen cards and quickly deploy them fraudulently at scale. And because it's increasingly easy to acquire and resell digital goods on marketplaces on the grey web—the part of the visible web dedicated to illicit activities—the size of fraud markets is growing quickly.

Rather than treating fraud as a customer service issue, we're increasingly seeing businesses deploy fraud prevention deeper into their products and systems to fight back. They're integrating fraud prevention with their payments and engineering teams for operational ease and are increasingly treating it as a product feature, aiming to minimize product friction for good customers while also still catching as many fraudsters as possible. That's vital for their conversion goals—33% of consumers say they won't shop again with online merchants that falsely declined them—and is why we've built tools into *Stripe Radar*, our fraud prevention tool, that allow businesses to customize fraud prevention to their circumstances to maximize conversion.

Will Megson,
Fraud Product Manager at Stripe

Will Megson helps develop Stripe's fraud protection tools, including Stripe Radar. He was previously the founder and CEO of Bouncer, which built card authentication technology to reduce fraud during online transactions and was acquired by Stripe in May 2021.

Vesta

Vesta is the only instant, end-to-end transaction guarantee platform for online purchases, delivering unparalleled approval rates, a better customer experience, and eliminating fraud for leading brands in telco, e-commerce, travel, and financial services. Using machine learning backed by 25 years of transactional data history, Vesta increases approvals of legitimate sales for its customers, while eliminating chargebacks and other forms of digital fraud, driving the true cost of fraud to zero and transferring 100% of the liability for fraud, including chargeback processing, so customers can focus on increasing sales. The company is headquartered in Portland, OR, with offices in Atlanta, Miami, Ireland, Mexico, and Singapore.

Vesta.io

How will fraudsters exploit return policies, and what will effective detection and prevention strategies look like?

Returns are a really tricky issue for e-commerce merchants to deal with. This is because merchants must have a flexible return policy to stay competitive, as well as remain conscious of fraudsters looking to take advantage of it. For example, during the pandemic, "item not received" type fraud has surged costing merchants large sums of their revenue. In fact, the National Retail Federation *reports* that during 2020 approximately $102 billion of merchandise purchased online was returned, with $7.7 billion (7.5 percent) labeled as fraudulent. A lot of return fraud has to do with shoplifting and then attempting to return the stolen items, or price tag switching, which entails purchasing an item at a lower price and then switching the tag out for a higher price and attempting to get a higher value return.

Despite these types of return fraud being most prevalent in brick and mortar, return fraud can also impact online merchants. Fraudsters will often create fake receipts or purchase them through nefarious websites and attempt to return items they never actually purchased. This abuse leads to lost revenue and increased operational costs from processing the fraudulent returns. The good news is that there are many ways for merchants to help prevent return fraud. The best way to prevent return fraud altogether is to prevent these bad actors from making these purchases in the first place, so having a very clear policy around returns is a great way for merchants to get ahead of fraudsters.

The only way to do that at scale is with a sophisticated machine learning fraud prevention solution that can analyze every transaction in real time by running it against hundreds of millions of historical transactional data points including customer phone numbers, IP addresses, credit card numbers, and so much more.

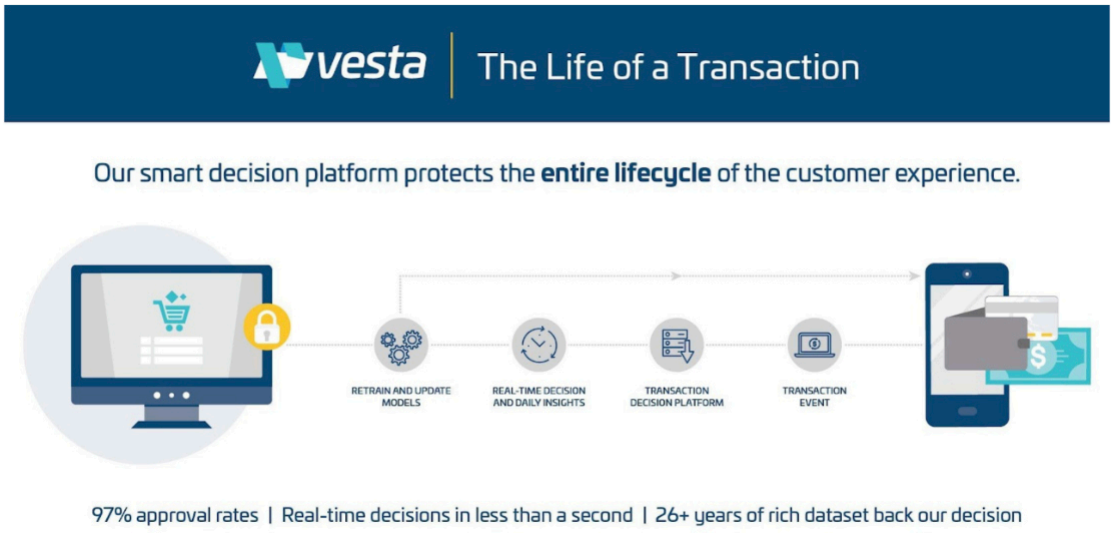
This type of deep link analysis allows merchants to make real-time transactional decisions that are rooted in data and proven to prevent fraud. And remember, those same bad actors will look to abuse your policy in many other ways, therefore merchants need to watch out for multiple fraud schemes. It's important to have a sophisticated fraud prevention solution that will stop all forms of CNP fraud while maximizing approvals of legitimate transactions.

What will be the biggest 2022 eCommerce fraud trend that is currently being overlooked?

Fraudsters are always on the lookout for new ways to hack and steal from both merchants and customers, and they're getting more sophisticated by infiltrating attacks with indirect linkage. What exactly does indirect linkage mean? Well, there are two primary forms of CNP fraud - attacks with direct linkage and attacks with indirect linkage.

When CNP fraud has direct linkage, it means there's some kind of red flag a merchant can look for to spot a fraudulent transaction. For example, if you notice five orders are placed from the same device within a five-minute window, it could be a sign that the orders are fraudulent, and the merchant should investigate further before approving the transactions or validating the purchase via SMS multi-factor authentication (MFA). Fraudsters also know what type of fraud is harder to detect, looking for weak links in the merchant's payment system as well as consumers' weak passwords in an attempt to steal their identity and credit card information. With indirect linkage, there is no easy sign merchants can look for, making it extremely difficult to identify and prevent.

We recently published our first ever *Global Card-Not-Present (CNP) Fraud Report* and found that fraudulent transactions with indirect linkage are on the rise, with the percentage of overall fraud with indirect linkage increasing steadily quarter-by-quarter throughout 2020. Additionally, we found the value of fraudulent transactions with indirect linkage is generally higher than those with direct linkage, making it an even more expensive and complicated problem for merchants to deal with. This leads us to believe that CNP fraud with indirect linkage is going to be a huge problem for the e-commerce industry in 2022. Merchants need to understand that not all fraud is created equal and stopping attacks with indirect linkage requires more sophisticated payment fraud prevention solutions.



Tan Truong,
Chief Information Officer at Vesta

A seasoned executive with 16+ years of experience and technologist by trade with two pending patents, Tan Truong builds and leads Vesta's technology, product, and operations teams to create a high-performance, innovative culture. With over a decade of spearheading large-scale Technology & Digital implementation across financial services under his belt, Tan develops Vesta's data science and machine learning capabilities to move beyond fraud detection and into fraud recognition as we approach a digital-first economy.

“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.

Contact Merchant Fraud Journal
Editor In Chief - Bradley Chalupski
bradley@merchantfraudjournal.com

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

hello@merchantfraudjournal.com

www.merchantfraudjournal.com

1-(888) 225-2909