



Cybersource+ experts:  
Fraud trends edition 2022

# The future of fraud

Securing growth in a changing world



# Contents

Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa Inc. does not make any warranty or representation as to the completeness or accuracy of the Information within this document, nor assume any liability or responsibility that may result from reliance on such Information. The Information contained herein is not intended as legal advice, and readers are encouraged to seek the advice of a competent legal professional where such advice is required.

# In a world of change, it pays to be ready for anything

The last few years have been like no other. Businesses worldwide have shown remarkable resilience, adapting fast to new opportunities caused by the eCommerce surge, constant shifts in consumer and fraudster behavior, and evolving government and regulatory demands.

Now it's time to prepare for what's next.

We brought together a team of experts from the Merchant Risk Council (MRC), Aite-Novarica Group and Cybersource to share their insights into the future of fraud, and help you develop strategies that not only reduce fraud, but can also bring more business in.

Learn more about:

1

How the pandemic changed fraud

2

The rise of the automated fraudster

3

What fraud trends to watch out for

4

4 steps to jumpstart your fraud strategy

# Meet our experts



## Tracy Kobeda Brown

### VP, Programs & Technology, Merchant Risk Council (MRC)

Tracy is an experienced executive whose expertise ranges from start-ups to Fortune 500 companies. Her skills span technology strategy, product design, engagement, gaming, mobile and information security.

In her spare time, she plays video games, and volunteers as a start-up coach and executive confidante. Having already met Oprah, her aspirations are to open an animal sanctuary, author a book, and build new technology solutions for law enforcement.



## David Mattei

### Strategic Advisor, Aite-Novarica Group

David has more than 15 years of experience in the payments industry designing, building, and launching fraud and dispute systems. His customers include merchants and financial institutions, giving him a unique and comprehensive perspective of their issues.

David's dream is to buy a one-way ticket to Europe, see all the sights, and return home only when he feels he's finished. He'd also like to buy the Italian village house where his grandmother was born.



## Mari-anne Bayliss

### Senior Director, Europe Regional Solutions, Cybersource

Mari-anne works with merchants in Europe to understand regional trends and ensure they're reflected in product development. She brings 20 years' experience in fraud prevention at a large U.K. retailer to her current role.

Outside of work, Mari-anne relaxes by cooking for family and friends. She's a passionate baker who daydreams about taking part in The Great British Bake Off.



## Martin Lee

### Director, Managed Risk Services, APAC, Cybersource

With more than 15 years of fraud prevention experience, Martin leads a team of experts across Asia Pacific. They're responsible for managing fraud strategies on behalf of clients who use Cybersource risk solutions.

Based in Singapore, but originally from the U.K., Martin is a huge soccer fan who spends most of his weekends enjoying late-night games.



## Mark Strachan

### Director, Global Services, Cybersource

Mark is a fraud risk professional with over 12 years' experience in the payment and banking industry. He works with merchants in sectors such as retail, digital and ticketing to develop strategies that reduce risk associated with fraudulent activity.

When not working, Mark can be found travelling to new places, hiking the hills, cooking at home, or indulging his love of theatre.

# 1 The pandemic changed fraud

“It’s amazing what’s happened with eCommerce sales growth. If you look at 2021, eCommerce sales grew significantly globally. If you take the pandemic out of the equation, it would have taken years for global eCommerce sales to reach the levels that we’re at right now.”

David Mattei  
Strategic Advisor, Aite-Novarica Group



Pandemic-related restrictions sent online sales soaring. However, this inevitably led to a global increase in fraud attacks on merchants. Recent research shows that around three-quarters of merchants reported increases in both fraud attempts and fraud rates by revenue, compared with pre-pandemic times.<sup>1</sup>

So it's no surprise that 9 out of 10 merchants consider managing eCommerce fraud very or extremely important to their overall strategy.<sup>2</sup>

## The consumer mentality changed

Consumers new to eCommerce may be unaware of, or not prepared for, the potential risks involved. With the shift to digital, fraudsters found new ways to commit crimes.

Social media became a new playground for many—with more than half a billion users joining social media platforms in just 12 months.<sup>3</sup> Although considerable effort has gone into educating people about the risks of online fraud and scams, it's easy to overshare personal details across social channels—a behavior that fraudsters jumped on.

**See [chapter 2](#) for more on how fraudsters use social media to carry out identity theft.**

There was also another important development: the increase in consumer-led fraud, namely friendly (or first person) fraud. Merchants rank friendly fraud as the most common type of fraud attack experienced during 2021, up from fifth in 2019<sup>4</sup> and estimate that around 1.2% of their accepted eCommerce orders turn out to be friendly fraud.<sup>5</sup>

**We look at friendly fraud and a similar type of fraud, policy abuse, in [chapter 3](#).**

<sup>1</sup> "2021 Global Fraud Report," Cybersource and MRC, 2021, p7

<sup>2</sup> "2021 Global Fraud Report," Cybersource and MRC, 2021, p6

<sup>3</sup> "Half a Billion Users Joined Social in the Last Year (And Other Facts)," hootsuite.com, July 2021

<sup>4</sup> "2021 Global Fraud Report," Cybersource and MRC, 2021, p17

<sup>5</sup> "2021 Global Fraud Report," Cybersource and MRC, 2021, p17

## Merchants adapted

During the pandemic, many fraud teams were under pressure as team members worked from home or were furloughed. At the same time as order volumes increased, fraud team resources were often limited.

**For some merchants, the experience resembled an extended peak season.** They struggled to staff fraud teams at a peak season level for that length of time. For the sake of the customer experience, some orders may have been let through that in the past would have been rejected. Meaning that, even as revenues increased, fraud rates may have done the same.

### The frictionless flow

**A frictionless experience became ever more important in the pandemic.** This was especially true for buy online, pick up in store (BOPIS) and curbside pickup purchases, where customers expect rapid fulfilment. When they can collect goods within an hour or two, there's no time for reviews before deciding whether to accept or reject an order—which potentially raises the fraud risk to the business.

“The pandemic upset what merchants knew historically about fraud. For example, the volume of friendly fraud isn't the way merchants were previously under attack, so they had to change their screening and review style.”

Tracy Kobeda Brown  
VP, Programs & Technology  
MRC



Pre-pandemic, we saw stores combine automated reviews with physical security measures at pickup, such as checking IDs and matching the payment card.

Now, we're seeing merchants use fraud screening to spot anomalies before an order gets to the pickup stage—combining machine learning to automate detection; global negative lists; and more sophisticated multi-variable velocities, such as multiple pickup locations being linked to a single identity.

**This is where a layered approach to fraud management comes into its own, a topic we explore in [chapter 4](#).**

“The struggle for revenues that some retailers experienced led to a ‘tug of war’ between fraud managers (who see their role as protecting against fraud) and those responsible for increasing revenues. How much risk would you accept in return for more revenue?”

Mari-anne Bayliss  
Senior Director, Europe Regional Solutions  
Cybersource





# Fraudsters kept pace

Even before the start of the pandemic, we were seeing a new kind of fraudster emerge: more organized and automated, and more likely to be operating as part of a group or ring than alone.

- **Focus has shifted away from fraud at the point of payment to stealing entire identities.** With more consumers going digital, fraudsters have been quick to exploit vulnerabilities—stealing data that allows them to set up entirely new accounts using real, fake or synthetic identities.
- **Fraudsters have quickly taken advantage of evolving fulfilment styles to circumvent fraud tools.** Take BOPIS, where no delivery address is captured, or fraudulent resale activity which has been designed to look like friendly fraud.

## The key message?

Manage risk beyond payment, and consider the end-to-end process—from account creation to delivery or receipt of goods, and even as far as the returns process. Validate where the risks lie to address weaknesses and maintain that optimal customer experience.

## 2 The rise of the automated fraudster

Identity theft and data compromise have become some of the biggest drivers of cybercrime, especially as fraudsters learned that stealing identities is worth much more than the fraud attack alone. The fraudster's traditional modus operandi is no longer enough: whereas in the past, they could generally count on being able to use stolen payment details for weeks, they no longer have that luxury. With online and mobile banking apps, accounts are checked several times a day, so stolen details may only work for a couple of hours.

Today's fraudsters are stealing identity data that allows them to set up 'clean' accounts which may remain usable for a number of weeks. We're finding:

- **Sophisticated approaches to identity theft** and the creation of fake accounts.
- **Increased automation:** with fraudsters incorporating the latest technology—using bots, chatbots and CAPTCHA bypassing technology, and even human click farms—to strike as soon as they spot new vulnerabilities.<sup>6</sup>
- **Fraud in plain sight:** Other fraudsters are leaving the dark web behind and taking their tech and tactics straight to social media.

<sup>6</sup> "Cybersecurity warning: 10 ways hackers are using automation to boost their attacks," ZDNet, March 2020

## Spotlight on: using social media to steal identities

Fraudsters try many routes to steal identity data, from hacking and social engineering to large-scale data breaches. Since the onset of the pandemic social media has provided fertile ground, as a wave of new users came on board.

We're seeing social media users:

- **Post information on their accounts** such as full name, date of birth, and photos of where they live or work
- **Make it easy for a fraudster** to glean their mother's maiden name by trawling through friends and family
- **Answer pop-up quiz questions which look harmless**, but may not be. For example, by asking which song was number one when you were born, fraudsters uncover your birth year and month. By combining this with your birth date (which we commonly include in social profiles), this discreet phishing attempt has revealed your full date of birth
- **Respond to fraudsters who pose as new contacts** asking personal questions about their favorite sport or the name of their first pet (often used as hints for forgotten passwords)

All this information can be captured by fraudsters with very little effort, enabling them to access a customer's online accounts, or build a complete customer identity for fraudulent use on other websites.

## 3 What to watch out for

There are a number of areas where fraudsters are likely to be especially active over the next year, and it pays to be vigilant.

### Account takeover and loyalty fraud—cause for concern

**New account origination fraud, new account fraud coupled with synthetic identities, and account takeover fraud**—when fraudsters illegally access or manipulate customer account data—all remain significant. Data breaches—in which millions of records containing personally identifiable information (PII) data can be compromised—are food for fraudsters to attack digital accounts.

Protecting against account takeover should form a critical part of your monitoring efforts to help you understand:

- Who is creating a new online account with you
- Who is logging in to an existing account
- Who is attempting to alter critical account information, such as password or shipping address

Data breaches and other forms of identity theft mean that a fraudster could have the right username and password to access an existing account; or a convincing combination of data to set up a new account. Ensure your fraud solution examines account events to determine the likelihood of genuine account access or creation.

“Some of the attack vectors we’ve seen recently are new twists on old ones. For example, new account fraud, in which synthetic identities are created to set up fake accounts that don’t relate to any particular person, but they’re being groomed, ready to be used down the road.”

David Mattei  
Strategic Advisor, Aite-Novarica Group



Loyalty fraud is on the rise and is a particular issue in the travel and hospitality sector. For most of us, opportunities to travel have been limited recently. Fraudsters are counting on the fact that, if we’re not travelling, we’re not checking our airline and hotel rewards programs as often as we used to. When fraudsters breach these accounts, they can quickly convert loyalty points into money.

The tools that protect your business and your customers against fraudulent account creation and takeover should also protect against loyalty program abuse.

“Until recently, travel restrictions meant that fraudsters saw little benefit in stealing and redeeming loyalty points. However, as travel opens up, they’re ready to take advantage. As well as using technology to protect against account takeover, it’s vital to educate customers on the importance of monitoring their accounts.”

Mark Strachan  
Director, Global Services, Cybersource



## 3 types of data theft used for payment fraud

We recommend addressing these forms of data theft as a priority. All can be used online for card testing and credential stuffing—which are features of many account takeover attacks these days.

1

### The use of malicious accessibility to steal data

**Fraudsters have long used techniques ranging from brute force attacks to phishing, smishing and malware to gain malicious access to data.**

As well as a rise in such attacks,<sup>7</sup> we're seeing fraudsters take advantage of the increase in people working from home. Fraudsters attempt to impersonate managers and directors by spoofing their email addresses, in order to persuade employees to provide credentials for access to network resources, and enabling the fraudsters to steal data.

2

### Dormant accounts: playing the long game

**Data breaches that took place in early 2020 allowed fraudsters to set up new online accounts just as the pandemic set in.** They hid among the flood of new accounts set up by genuine customers shopping online for the first time.

In many cases fraudsters didn't use those accounts until much later, on the assumption that transactions made on older accounts are less likely to be fraud screened. Sophisticated fraud tools can identify and block these accounts.

3

### SIM swapping on the rise as strong customer authentication kicks in

**SIM swapping, also called SIM hijacking or SIMjacking, allows a fraudster to gain control of an individual's mobile phone account.** Armed with information gleaned from social media or stolen in a data breach, the fraudster poses as the account owner and persuades the mobile phone company to move the account from the owner's SIM to a SIM controlled by the fraudster.

The fraudster can then intercept SMS messages containing one-time passwords (OTPs) or PINs that are used for strong customer authentication (SCA) when buying online. The rollout of PSD2 SCA in Europe means more reliance on OTPs and PINs, and a likely increase in SIM swapping attacks.

<sup>7</sup> "INTERPOL report shows alarming rate of cyberattacks during COVID-19," INTERPOL, April 2020

## Spotlight on: **the rise in friendly fraud and policy abuse**

Friendly fraud (also known as first-party fraud) takes place when a customer buys a product or service online with their payment card, then contacts their card issuer to dispute the charge—claiming, for example, that the item didn't arrive or arrived damaged.

It can also happen when a customer struggles to navigate a merchant's returns and refund process, or a refund simply takes too long.

“Handling and disputing friendly fraud creates a lot of operational work for the merchant. It's an unwelcome challenge that also impacts on revenue loss and forecasting. Nothing about friendly fraud is actually friendly.”

Martin Lee  
Director, Managed Risk Services, APAC  
Cybersource

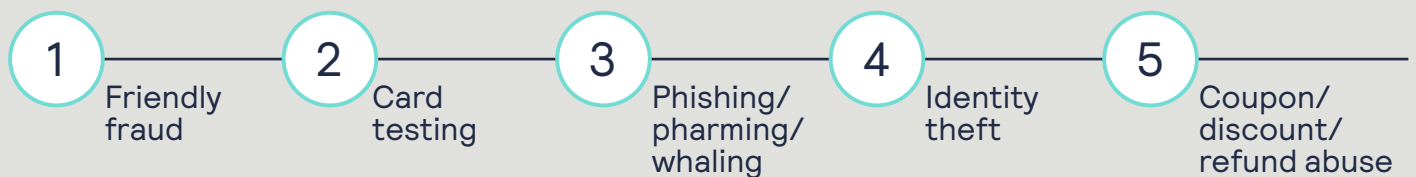


Our experts point out that, in the past, friendly fraud was generally about people being opportunistic—perhaps taking advantage of a weakness in the merchant’s processes.

When a merchant identified a case of friendly fraud and challenged the customer, they usually didn’t do it again. But friendly fraud is growing and evolving—perhaps because the economic effect of the pandemic has made consumers more entrepreneurial; and there’s not much in the way of a penalty for falsely claiming a package didn’t arrive. Merchants globally say friendly fraud is now the most common fraud attack they experience—closely followed by card testing, phishing and identity theft.

## Top 5 fraud attacks experienced by company size

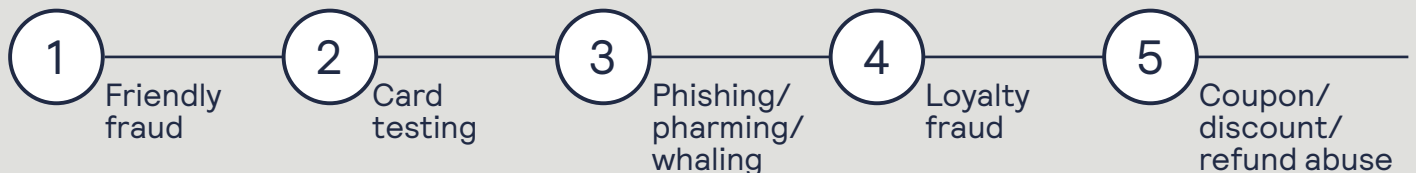
### SMB



### Mid-Market



### Enterprise



Source: Global Fraud Survey Results 2021, Cybersource and MRC, 2021



### Let's look at some of the key changes we're seeing in friendly fraud:

- **Family fraud** is a form of friendly fraud that stems from sharing devices among family members, any of whom may make an in-app purchase without the cardholder's permission. The cardholder may go the dispute/chargeback route to reclaim the funds.
- **Friendly fraud relating to digital goods** can be hard to prove because there's no signature or other proof of delivery. Merchants need to gather additional data to help them prove to the bank that the customer did place the order. Device fingerprinting, geolocation data and behavioral biometrics are useful tools here.
- **Friendly fraud may increasingly be related to fraudulent reselling.** If an organized fraud ring pulls off enough friendly fraud, it could culminate in the online resale of what are effectively stolen goods.
- With countries reopening, consumers have gone on larger than normal spending sprees. This urge to spend is known as revenge spending.<sup>8</sup> It can **contribute to buyer's remorse**, which may make customers more likely to dispute the transaction.

There's a close link between friendly fraud and policy abuse—which includes coupon, discount and refund abuse, the fifth most common type of fraud attack globally.<sup>9</sup>

**Policy fraud includes:**

- **Customers returning items that are different from the ones they bought.** This may be quite flagrant—for example, a fake designer handbag sent back in place of the genuine item.
- **Customers returning BOPIS purchases** and requesting a refund to a different card.
- **Professional refunders' openly advertising their services** on social media sites. They position themselves as experts in return policies with bespoke strategies to ensure refunds are approved. Once a refund has been processed, the professional refunder charges a fee for their services, which may be 20% of the value of the item.

In response to its rise over the past two years, **80% of merchants globally have a formal approach for combating friendly fraud.**<sup>10</sup> Most have opted for a multi-pronged strategy with a range of tactics including customer notifications, clear payment and returns policies, and various verification measures that check and confirm customers' identities.

The rise in friendly fraud is challenging the sanctity of negative lists, meaning they need to be regularly revisited and cleaned.

**Consider using additional screening technology**—such as Cybersource Decision Manager's Identity Behavior Analysis, which draws on an extensive global negative list—to help make the right accept/reject decisions.

“Friendly fraud is a real problem for digital goods merchants (such as online games), who are telling Aite-Novarica Group that up to 75%<sup>11</sup> of their chargebacks are due to it, which is staggering.”

David Mattei  
Strategic Advisor, Aite-Novarica Group



<sup>9</sup> “2021 Global Fraud Report,” Cybersource and MRC, 2021, p16

<sup>10</sup> “2021 Global Fraud Report,” Cybersource and MRC, 2021, p18

<sup>11</sup> “Improving the Dispute Experience: Transparency Is Power,” Aite-Novarica Group, May 2020

## Spotlight on: the increased impact of regulation

Merchants worldwide report that keeping up with regulations or industry rule changes is the #1 fraud management challenge they experience—closely followed by responding to emerging fraud attacks.<sup>12</sup>

**The rollout of PSD2 SCA is a good example**, affecting businesses selling into or within Europe. Although the strong customer authentication (SCA) requirement is designed to protect electronic payment transactions with two-factor authentication, fraudsters try to find ways around regulations. The increase in SIM hijacking is one of a number of routes fraudsters may take, as they attempt to gain access to the OTPs and PINs used for SCA.

**PSD2 SCA led to increased adoption of EMV® 3-D Secure<sup>13</sup> (3DS)** as a way of complying with the SCA requirement. Merchants who work closely with their fraud solution provider have been able to choose when to invoke or suppress EMV® 3DS within the customer payment experience; and how to handle transactions that may qualify for exemptions or be out of scope for SCA.

**Those not directly affected by PSD2 SCA are watching to see what happens** and the role played by EMV® 3DS in mitigating eCommerce payment fraud, as a regulation that works well in one region could ultimately get adopted elsewhere.

<sup>12</sup> "2021 Global Fraud Report," Cybersource and MRC, 2021, p19

<sup>13</sup> EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC.

## 4

## Building a fraud strategy that gets more business in

There's plenty you can do to address the automated fraudster, future-proof your fraud strategy, and make the incremental changes that help not only to stop the bad guys, but also to get more business in.

**Action plan:** 4 steps to jumpstart your fraud strategy >

## Step 1. Take a layered approach to fighting fraud

No single tool can do everything you need to fight fraud. A layered approach uses multiple tools across the customer experience. Ensure your fraud solution combines:

**Account-level tools. Start screening for fraud at account origination.** To identify and prevent account takeover, you need to spot the difference between genuine and high-risk events. This includes account creations, logins and updates, and account takeover fraud.

Solutions such as Cybersource's Account Takeover Protection include features like device fingerprinting, behavioral biometrics, and physical biometrics, as well as one-time passwords (OTPs).

**Pre-screen transaction tools. Catch orders associated with identity theft, card testing and credential stuffing** before they result in declined authorizations. Pre-screening tools can be used upstream during processing, to detect fraud before authorization.

They combine machine learning and your own policies to block fraud—helping stop card testing attempts before they happen, and before authorization fees are incurred.

**Payment transaction-level tools.** Over half<sup>14</sup> of merchants recently surveyed by Aite-Novarica Group still rely on a rules-based approach to manage online payment fraud.

**To deal with today's automated fraudsters, use advanced machine learning models** that evaluate historical transaction data to find patterns and inform new fraud strategies—with access to global data and industry insight.

**Orchestration layer for tool configurations. Use machine learning to automate risk calibrations,** reduce the load on fraud teams, and cut down on reviews. Sophisticated analytics and reporting help optimize these tools and enable self-tuning, so you can focus on your business—not on fraud.

“The rate at which fraud is evolving means that traditional fraud screening rules are too static to be enough on their own. You need to find the right balance between rules, AI, machine learning, and manual review.”

Mari-anne Bayliss  
Senior Director, Europe Regional Solutions  
Cybersource



<sup>14</sup> Aite-Novarica Group quantitative survey of 756 mid-size and large eCommerce merchants in North America, Europe, and Asia-Pacific, 2021

## Step 2. Get your fraud/friction balance right

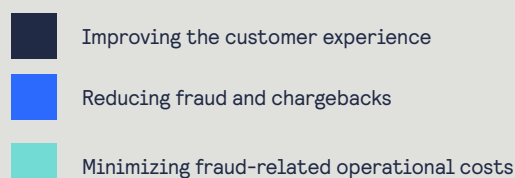
Despite the increase in attacks and lost revenue, half of merchants say that improving customer experience is their top priority when managing fraud.<sup>15</sup>

**Carefully monitor the consumer experience to avoid adding too much friction.** And be friction appropriate. Start by applying low- or no-friction tools (such as device fingerprinting and behavioral biometrics) that run in the background.

When you see something suspicious step up to another identification method, using machine learning and AI, to identify the person on the other end of the transaction; or engage that person in a task, such as entering an OTP.

That way, you can maximize your approval rates and minimize fraud losses, while delivering an amazing customer experience.

### % selecting most important fraud management priority



Source: Global Fraud Survey Results 2021, Cybersource and MRC, 2021

“Merchants are concerned about the customer experience because friction and cart abandonment are two things they try to avoid at all costs. But you really can’t talk about the experience unless you bring the fraud organization into the conversation, since it’s the fraud strategies and the tools deployed that have a direct impact on CX.”

Martin Lee  
Director, Managed Risk Services, APAC  
Cybersource



<sup>15</sup> “2021 Global Fraud Report,” Cybersource and MRC, 2021, p21

## Step 3. Make the fraud department a key player in business decisions

Managing fraud is no longer regarded as an operational function that cuts fraud rates.

**Today's fraud managers are increasingly targeted on transaction approval rates**, reducing operational costs, championing automation and dynamically applying authentication.

They have a key role in understanding changes in customer behavior and reformulating sales strategies. So it's important to have fraud teams involved at the beginning of business planning—not after.

“Elevate the fraud department and make it a co-partner in the overall business. Looking at successful organizations these days, the business line, marketing function, finance, operations, and fraud teams all come together to work cohesively and collaboratively.”

David Mattei  
Strategic Advisor, Aite-Novarica Group



## Step 4. Put the appropriate metrics in place

Be sure to apply the right metrics and continuously improve fraud strategies by leveraging your data—to help you boost revenues.

**As well as fraud losses, you'll need to look at other metrics like:**

- Your customer insult rate (denying good customers—which you may hear about from your operations or call center team)
- Your approval rates (which may come from your line-of-business or operations teams)

That way, you can learn from what's gone before and feed the information back in to your fraud strategy, to help maximize your sales and approval rates, and cut your fraud losses.

At the same time you'll do a better job of measuring the overall performance of the fraud team.

“If a merchant has a high fraud/sales ratio, card issuers can get stricter. Merchants in this position need to become more strategic about their overall fraud rates. For example, consider moving fraud screening ahead of authorization to have a stronger impact on authorization rates.”

Mark Strachan  
Director, Global Services, Cybersource





# Readying your teams for change

Fraud teams have had to react fast to support and advise through the pandemic. Their role continues to evolve, and new KPIs are emerging.

Regardless of what happens with the pandemic, **fraudsters will continue to aggressively look for new vulnerabilities to exploit**, just as they always have. For example:

- A move to hybrid working models could drive increased doorstep fraud.
- Vaccination passports could become an additional layer of identity, but also a magnet for fraud. We're already seeing rampant sales of vaccination passports on the dark web at prices as low as \$12.<sup>16</sup>

## Prepare for what's next

**Re-baseline data from the pandemic-influenced period.** Look at order volumes to consider what proportion can still be classed as pandemic impact.

- To reduce friction associated with authorization, go beyond chargeback rates and review risk analysis targets. You may let an acceptable amount of fraud through, in order to safely remove purchase barriers.
- If your business is planning to introduce new digital capabilities, such as mPOS, digital check-in or contactless deliveries—all of which can enhance the customer experience—allow enough time to assess the fraud risks they may bring.

“Look at emerging technology and assess its suitability to address the components of your fraud experiences that are impacting revenues. Prioritize projects according to ROI and the TCO of adding them into your fraud practice. And if you haven't already done so, talk to your C-suite to get appropriate funding to improve the customer experience and protect revenues.”

Tracy Kobeda Brown  
VP, Programs & Technology  
MRC



<sup>16</sup> “Booming market for fake COVID-19 vaccine passports sparks alarm,” Reuters, April 2021

## How Cybersource can help

Our fraud and risk management solutions put as much emphasis on accepting genuine customers as on stopping fraud, so you can focus on your business.

### Combine machine learning and risk-based strategies for better results


**Machine learning has been a core part of our fraud solutions since day one**—and we've been upgrading ever since. Now a Visa solution, we deliver considerable advantages with our combined strength, size and scale.

- **Real-time automation analyzes hundreds of data points** against intelligence from Visa and Cybersource data, generating a powerful risk score that automatically accepts or rejects transactions, blocking fraudsters and staying ahead of attacks.
- **From account login to payment acceptance, we automate risk detection** to help you speed fulfilment and boost your revenue flow, while keeping friction low and customer satisfaction high.

### Get more out of your business

**Get the insights and control you need to find the right balance** between reducing fraud rates, improving approval rates and lowering costs.

- **Since one size does not fit all**, we secure your business with a multi-layered defense—from Account Takeover Protection, through to Cybersource Decision Manager—all backed by the power of machine learning.



# Are you ready to get started?

We can help you secure  
growth in a changing world.  
Get in touch today to find  
out how.

[cybersource.com](https://cybersource.com)

>> [Contact us](#)

Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa Inc. does not make any warranty or representation as to the completeness or accuracy of the Information within this document, nor assume any liability or responsibility that may result from reliance on such Information. The Information contained herein is not intended as legal advice, and readers are encouraged to seek the advice of a competent legal professional where such advice is required.

