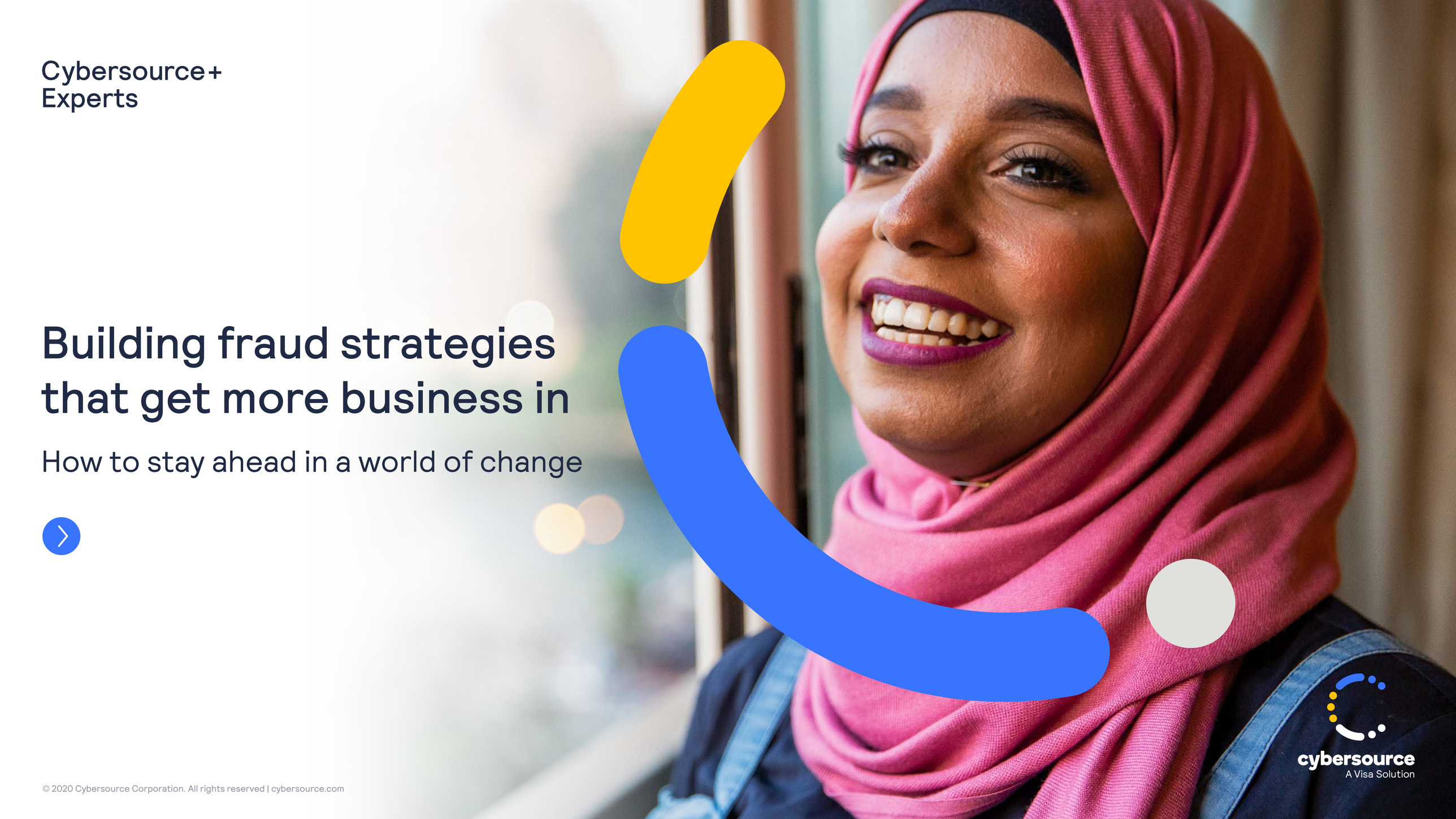
Cybersource+
Experts

Building fraud strategies that get more business in

How to stay ahead in a world of change



cybersource
A Visa Solution

Contents

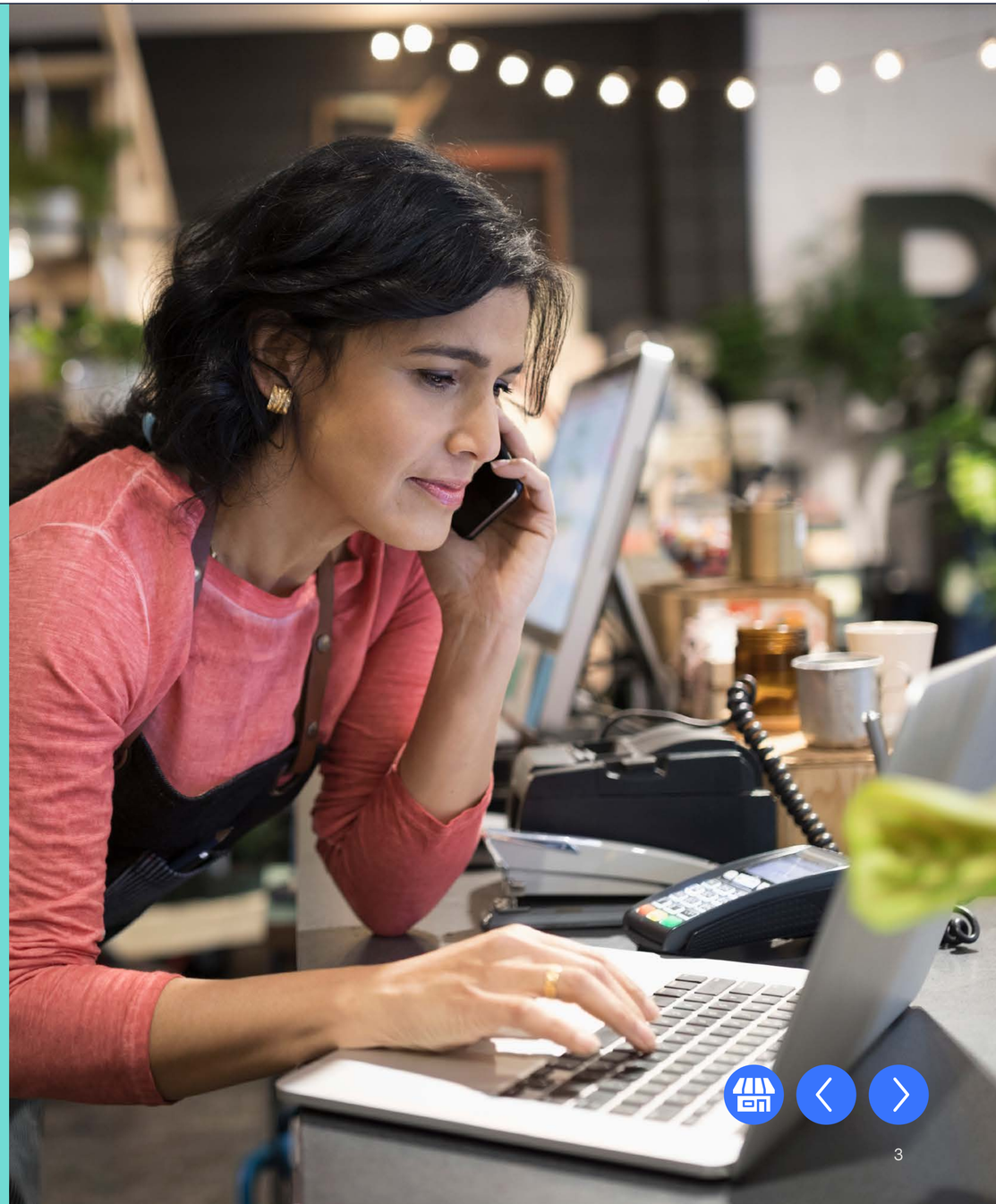
In a world of change adaptability is everything

As the COVID-19 pandemic caused a surge in online shopping and some truly innovative business responses, fraudsters too looked for ways to adapt their behavior.

We've got you covered. To help prepare for what's next, we brought together a team of specialists from the Merchant Risk Council (MRC), Decoded and Cybersource to share their insights, and help you jumpstart your fraud strategy.

Read on to learn:

1. How merchants have responded to the changing fraud landscape
2. The top priorities for fraud teams as we gear up for the future
3. How you can build a fraud strategy that not only stops bad orders, but helps get more business in



Meet our experts

Una Dillon

Managing Director, Europe, Merchant Risk Council (MRC)

Una's role at the MRC gives her unique insight into merchants' challenges and priorities in the evolving world of eCommerce. Her extensive experience includes payment regulation, fraud prevention and financial services strategy.

Chris Monk

Director of Business Operations, Decoded

Chris combines a passion for technology, software development, cybersecurity, data science and the internet of things with a zeal to educate. He's responsible for the delivery of Decoded's executive technology education services in EMEA and APAC.

Andrew Naumann

Vice President, Product Management, Cybersource

Andrew is responsible for the vision and strategy for Cybersource fraud management solutions. As well as product managers and decision scientists, his cross-functional team includes risk analysts who develop fraud strategies for key clients.

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 UK retailer to her current role.

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 to reduce risk associated with fraudulent activity.

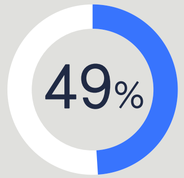
When the world around you changes, you can't afford to stand still

We are operating in constant change. Customers alter their behavior and revise their expectations. Technology advances. New regulations come into force.

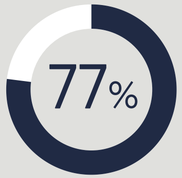
Unpredictable external factors bring change too. Take the COVID-19 pandemic: lockdowns and government guidance caused a big shift to online shopping, encouraging a fair few consumers to buy online for the first time ever.

As Chris Monk from Decoded puts it: "COVID-19 has done more for eCommerce adoption than any other single thing in the past 10 years."

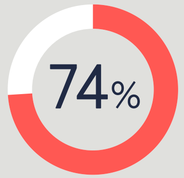
COVID-19 drives a shift to eCommerce



of consumers globally say they're shopping more online than before COVID-19[1]



of UK consumers now do at least part of their grocery shop online[2]



of people in the UK across all age groups now feel comfortable buying online since the COVID-19 outbreak[3]

"Keeping the balance right between a good fraud prevention strategy and the consumer experience is always a challenge."

Una Dillon, MRC

[1] Source: Bazaarvoice "Pandemics and presents: A look at how consumers plan to shop for the holidays in 2020"
[2] Source: Waitrose "How Britain Shops: Online Food and Drink Edition"
[3] Source: Bazaarvoice "Behavior that sticks: Understanding the long-term shopping trends driven by COVID-19"

Stores whose previous business was mainly or exclusively face-to-face had to embrace eCommerce very quickly. Setting up websites. Getting logistics operations in place. And implementing payment platforms and fraud detection systems for card-not-present (CNP) transactions.

“The fraud rate for these merchants was likely to increase owing to their lack of experience and how fast they had to deploy. And there’s always going to be a higher rate of fraud with CNP transactions than with point-of-sale (PoS) transactions,” says Mari-anne Bayliss from Cybersource.

And as her colleague Mark Strachan points out, fraudsters are smart and flexible: “They keep up to date with the evolving eCommerce landscape and adapt their behavior, tools and techniques accordingly.”

“Fraudsters will always customize their attacks to make them relevant to whatever’s happening in the world.”

Mark Strachan, Cybersource

How has the pandemic changed fraud?

Mark explains that the changes observed have been less about new types of fraud, and more about fraudsters rapidly adapting their practices to take advantage of the new situation. Fraudsters have, for example, carried out COVID-19–themed phishing and smishing attacks to steal account credentials that can be resold or used in account takeover and loyalty fraud attacks.

And, as expected, they've moved quickly to exploit the pandemic-driven increase in online shopping. "It's inevitable that online fraud would increase because criminals will always go where the money is," says Chris.

The MRC's Una Dillon picks up on the challenge this creates for businesses that haven't traditionally had a strong eCommerce channel: "It's been a huge change for a lot of merchants, especially those with physical stores as well as online channels, who've seen a flood of new online customers. And while that sounds like a good problem to have, it makes things more difficult in terms of fraud prevention, as fraud teams are faced with fraudsters hiding in among the good customers."

Some noticeable changes in fraudsters' behavior have been:

1. Taking advantage of contactless and other socially distanced delivery options (that don't require a customer signature) to commit fraud
2. Increased buying of digital goods, such as eGift cards, using stolen card details to avoid the longer window for fraud screening associated with physical goods
3. More account takeover and loyalty fraud attacks

Friendly fraud — already ranked 5th out of the top 10 fraud attacks experienced[4] — has increased. Una's view: "I think that spending extended periods at home in front of their computer has led some people to make more impulse purchases online. They may then experience 'buyer's remorse', or simply decide they don't want the item anymore."

Friendly fraud — also known as chargeback fraud or first-party fraud — can also happen when a customer struggles to navigate a merchant's returns and refund process, or a refund simply takes too long.

Whatever the reason behind friendly fraud, Mari-anne from Cybersource advises: "To deal well with friendly fraud means spotting it fast and taking action. It's a genuine customer doing something dishonest — there's no sophisticated strategy behind it."

Mari-anne Bayliss, Cybersource

What is friendly fraud?

A customer makes a purchase online for a product or service with their payment card and then contacts their card issuer to dispute the charge. This type of fraud is often referred to as friendly fraud because the customer will make claims that seem believable and honest.

Source: Verifi.com

[4] Source: Cybersource: Masters of Balance, 2019 Global eCommerce Fraud Management Report

How have businesses responded?

"Being adaptable involves keeping up with the latest fraud trends. Knowing what fraud is out there is the first step to preventing it," says Una. "It's good to broaden your outlook — speak with external experts, acquire intelligence from merchant groups, and build networks to share knowledge."

Businesses should also use chargeback reports from card issuers, available from acquirers, to gain insight into transactions that have been reported as fraudulent. Understanding the reason for each chargeback claim can help a business recognize risk more effectively.

"The pandemic has been a huge learning curve for some merchants, and criminals will be aware of this. They will look for the weak spots."

Una Dillon, MRC

During the pandemic, we've seen merchants make rapid adjustments to their fraud strategies to:

1. Avoid chargebacks and other issues associated with increased fraud
2. Accept more genuine orders
3. Maintain a great shopping experience for genuine customers

The role of machine learning in fraud detection

Businesses need to use machine learning (ML) intelligently to enhance both the customer experience and their fraud strategy. Una points out that merchants have access to huge amounts of data about consumer behaviors, activity and velocity levels — all of which can be measured. "So why not use the tools? It just makes sense," she says.

Although ML is a powerful technology, it's only as good as the data it consumes and the human-set rules it works to. So it's unlikely that a tool based exclusively on ML could pick up quickly enough on the changes in consumer and fraudster behavior caused by a situation like the pandemic. "A business that relies exclusively on ML in such a context could experience high rates of fraud and chargebacks, or low levels of customer satisfaction as too many good orders are rejected," says Mark.

Instead, businesses should consider using a fraud screening tool that's backed by experts who can help with fraud strategy creation and adaptation. As Mari-anne explains: "In any fast-changing time, you need human intervention to carry out day-to-day analysis of new trends. It's never one thing alone that will solve the problem — you need to take a layered approach to fraud screening."

> "The disadvantage of ML is that it's backward looking. Working alone, it may not adapt as readily as a human being who can quickly understand a new context, such as COVID-19, and react promptly to changes in patterns."
>
> Andrew Naumann, Cybersource

Spotlight on account takeover and loyalty fraud

Account takeover and loyalty fraud attacks typically start when fraudsters steal account credentials in a data breach or a phishing or smishing attack. Counting on the fact that many people reuse passwords, a fraudster then uses those stolen credentials to try to log in to customer accounts on other websites.

Once logged in, the fraudster will steal or misuse whatever's stored in the account: personal information, payment details, vouchers or loyalty points. Chris notes that loyalty points can be extremely valuable: "Because I've traveled so much for work, my airline loyalty account is probably worth more than my bank account!"

"Fraudsters will use loyalty points to buy high-value items like first-class flights or five-star hotel rooms, then sell them on," says Una. "That's why the Merchant Risk Council encourages its members to treat their loyalty programs as they would cash."

"People know that reusing passwords is a bad idea but it doesn't always stop them. Almost all of us know someone who's been a victim of account takeover."

Chris Monk, Decoded

The global loyalty management market was valued at USD 3.2 billion in 2019, and is expected to reach a value of USD 11.4 billion by 2025[5]

[5] Source: Loyalty Management Market — Growth, Trends and Forecasts (2020–2025).

Customers of an online business affected by account takeover or loyalty fraud may lose trust in the brand and walk away from it. The business may also have to deal with financial losses, including customer refunds, chargeback fees and inventory loss. “As merchants look to rebuild business and deal with the pandemic-driven recession that’s on the cards, these are risks they’ll want to avoid,” says Mark.

The most effective approach to preventing account takeover and loyalty fraud involves monitoring account activity to detect and block fraudsters before they can carry out any transactions. From a behavioral point of view, automated login attempts using a credential stuffing tool — a feature of many account takeover attacks these days — look quite different from logins by genuine account-holders.

Using a specialized account takeover protection solution can help. “Your solution should be able to distinguish between genuine and fraudulent behavior by monitoring account events — creation, login and update — for suspicious activity, and factoring in data relating to things like email addresses and devices used,” says Mari-anne.

What is credential stuffing?

Credential stuffing is the practice of using stolen login information from one account to gain access to accounts on a number of sites through automated login. The exploit can allow hackers and those buying stolen credentials to access not just the accounts from the sites they are stolen from, but any account where the victim uses the same password.

Source: WhatIs.com

Top takeaways

In times of rapid change, businesses need to:

1. Keep up to date with evolving fraudster and customer behavior — gleaning intelligence from external as well as internal sources
2. Be ready to adapt their fraud screening techniques accordingly
3. Combine machine learning with human insight to combat fraud more effectively
4. Consider deploying a specialist tool to help combat account takeover and loyalty fraud

Build a fraud strategy that helps capture more revenue

The impact of the pandemic on merchants' revenues has depended to a large extent on what they sell. Vendors of essential products and providers of streaming services have generally seen revenues increase, and will want to maintain those levels. On the other hand, travel and tourism operators have been among the worst affected, and will want to restore revenues as quickly as possible.

"Either way, merchants will want to ensure their fraud strategy is tuned to accept as many good orders as possible — without losing sight of the need to minimize fraud," says Mark.

"We're seeing merchants' preoccupation change from pure fraud management to revenue capture."

Andrew Naumann, Cybersource

Know your genuine customers. And treat them right.

In the digital economy speed and convenience mean everything. Businesses need to make a good impression on new customers. And given that the shift to online shopping looks likely to be the 'new normal', merchants should do their best to capitalize on it. Ensuring a secure, frictionless payment experience for genuine customers is critical, so you need to able to recognize them, as Andrew explains:

"You have to take into account, for example, that if an order has to be shipped within 24 hours, there's limited time for manual review. Or if card details are stored in customers' accounts (also known as card on file), there's a risk of account takeover and fraudulent purchases being made. It's why the device fingerprint has become so important: a merchant has to know who the customer is all the time."

Advanced technology has a role to play here, with different methods employed to create a unique customer ID.

"Voice recognition, haptic recognition, typing habits all help to create a unique ID for a customer — and get away from passwords."

Chris Monk, Decoded

What is a device fingerprint?

Device fingerprinting is a way to combine certain attributes of a device — like what operating system it is on, the type and version of web browser being used, the browser's language setting and the device's IP address — to identify it as a unique device.

Source: Digiday.com

Know your genuine customers. And treat them right.

(continued from previous page)

Fraud detection and the customer experience are two sides of the same coin, and each business will make its own decision about how to balance them. But focusing only on stopping fraud could affect a lot of genuine customers by providing a less-than-great customer experience. To avoid that pitfall, Mark advises merchants to treat good customers with different rules than those used for suspicious-looking purchases.

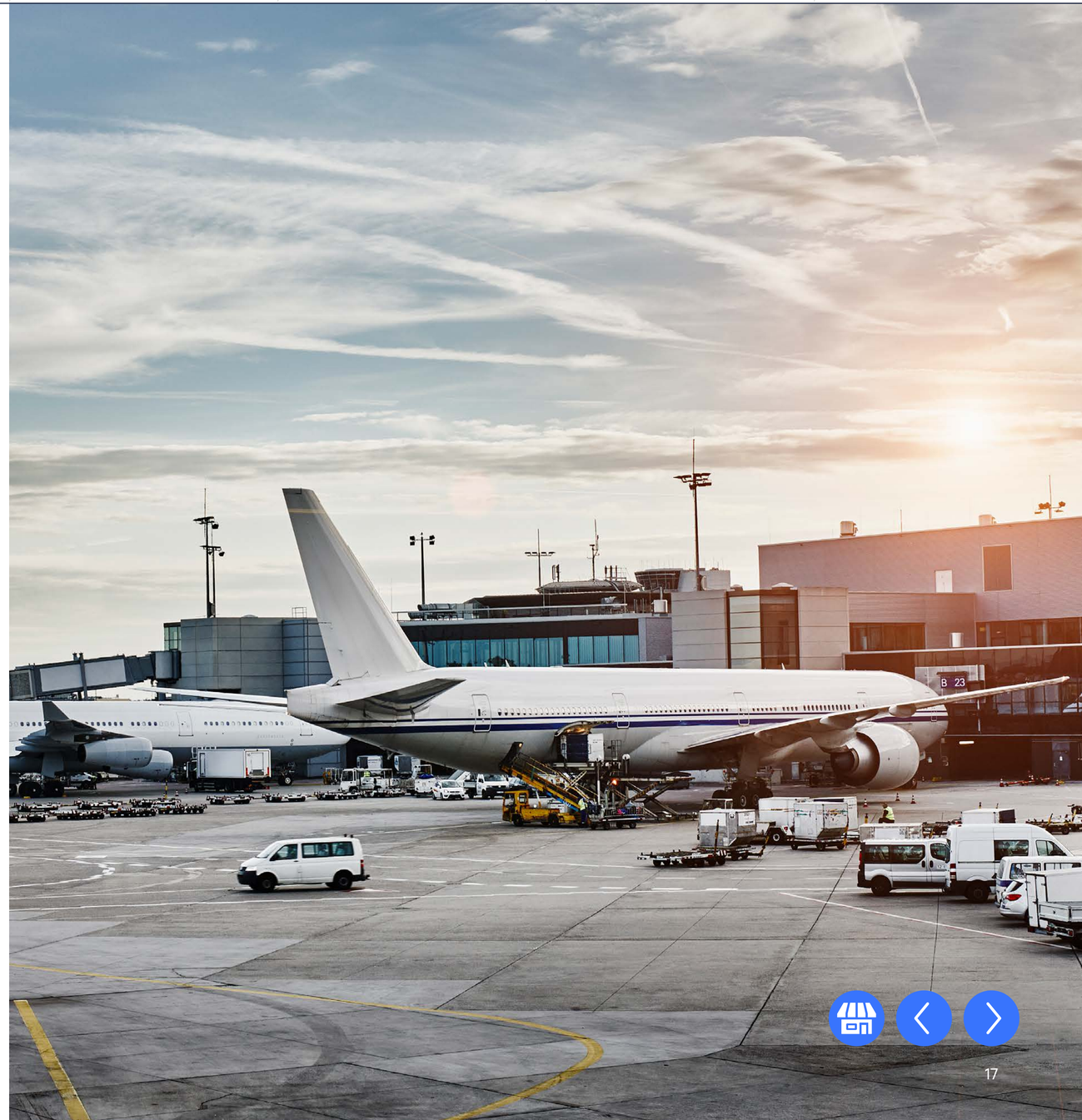
“You need to combine a high-quality detection system with knowledge about normal sales, and make a choice based on the numbers,” he says. “That involves using scoring models that take account of positive customer behavior in order to streamline the experience for genuine customers and make the fraudsters stand out.”

For transactions that exceed a specified risk threshold, a business will need to add human insight — such as an understanding of the customer and local knowledge — to make decisions about how to deal with a risky order.

Help your customers buy what they need

Embedding your fraud detection and prevention system at the core of your business decision-making can help you adjust — and enforce — your business policy to support good customer experience, especially in times of turbulence. Andrew explains how Cybersource supported businesses doing this during the pandemic by helping them make creative use of tools they already had:

“We helped a supermarket to ration the volume of a given product to ensure fair shares for all consumers. And we helped airlines accept one-way bookings for repatriation flights — instead of treating them as potentially fraudulent transactions — so that people could get back home when lockdowns and quarantines came into force.”



The next step: optimize authorization

VisaNet data shows that issuers declined 13.07% transactions globally in the period of October 2019 to September 2020[6]. This represents a potential loss of revenues for merchants as some of those declined transactions would have been good orders.

To reduce the number of good orders being declined, merchants should look at how they can help issuers make more informed decisions. For example, if a merchant screens transactions for fraud before sending them, the issuers will receive better quality transactions that they're more likely to accept.

As Andrew explains: "Merchants actually have more data about transactions than issuers do. Sharing some of that data with issuers will provide them with more information on which to base decisions. This is where EMV® 3-D Secure can help."

EMV® 3-D Secure (EMV® 3DS) allows a merchant to share 10 x more data with the issuer (135 data elements in total) compared with 3DS 1.

"Card issuers decline more CNP transactions than in-store. So there's an opportunity for merchants to close that gap and increase their revenues. That involves merchants boosting issuers' confidence to authorize more of those transactions for payment."

Andrew Naumann, Cybersource

[6] Source: VisaNet Global issuer decline rate in the period of 1 October 2019 to 30 September 2020

Top takeaways

To build a fraud strategy to capture more revenue, businesses should:

1. Focus on recognizing good customers and creating a great shopping experience for them
2. Make it easy for customers to buy the products and services they need
3. Look at recapturing lost revenue by enabling card issuers to make more informed decisions about transactions

Gear your business up for the future

Merchants' coming fraud management priorities will depend on the maturity of their current strategy.

Understanding and combating fraud will be an ongoing concern, as will ensuring their operations are cost effective. But businesses shouldn't allow their focus to drift from driving revenues and retaining good customers. "A fraud screening tool like Cybersource Decision Manager will help merchants get the balance right, especially in challenging times like these," says Andrew.

Data also has a critical role to play in a successful fraud strategy: "As well as investing in the right tools, merchants need access to the right data (and enough of it). Your own data is good but the ability to see what's happening elsewhere — and to learn from other merchants — will help you react faster to change," advises Mari-anne.

Mark suggests that businesses should ensure their business strategy is aligned to consumer buying patterns, their chargeback processing is effective, and that they continue investing in their fraud teams. "Throughout this challenging period, fraudsters will expect skeleton staffing and reduced budgets, and will take advantage of merchants who don't keep a close eye on fraud," he warns.

"A fraud screening tool like Cybersource Decision Manager will help merchants get the balance right, especially in challenging times like these."

Andrew Naumann, Cybersource

Optimize for PSD2 SCA

PSD2 is the revised European Payment Services Directive. The associated strong customer authentication (SCA) requirement means that some payment transactions — when both issuer and acquirer are in the regulated area (European Economic area (EEA), UK and Gibraltar) — will need two-factor authentication. If the issuer can't authenticate a transaction, it may be declined.

Some transactions will be out of scope for SCA:

- Those in the mail order/telephone order (MOTO) channel
- Those initiated by merchants (such as direct debits)
- One-leg-out (OLO) transactions (when the issuer or acquirer is outside of the regulated area)
- Recurring transactions with a consistent amount once the first one has been authenticated

As well as increasing security for online payments, PSD2 SCA aims to optimize the customer experience. That's why some transactions that are in scope for SCA may be exempted from authentication by acquirers or issuers. One way they may make this decision is by using transaction risk analysis (TRA) on lower-value transactions.

"The scale of change with SCA is big. Merchants need to familiarize themselves with exemptions and out-of-scope transactions, and be ready to support compliance."

Mari-anne Bayliss, Cybersource

Optimize for PSD2 SCA

(continued from previous page)

"If you don't screen for fraud, you could expose your business to it.

For one thing, you'll need to protect transactions that are out of scope for SCA, which could become a target for fraudsters once SCA comes into force."

Mari-anne Bayliss, Cybersource

"Merchants must do their best to identify in-scope transactions that may be exempted from authentication," says Andrew. "Although only acquirers and issuers can exempt transactions, merchants need to be in constant conversation with their acquirers about possible exemptions, and about how to navigate the legislation and establish an SCA strategy."

Merchants will want to keep any perceived SCA friction for customers to a minimum. "This is why a move to EMV® 3-D Secure is recommended. In particular, it will ensure a better SCA experience on mobile devices — which is important as many people are shifting to shopping on their mobiles," says Mari-anne.

And if any merchants are wondering why they'll need to continue screening for fraud once SCA comes into force, Mari-anne has the answer: "If you don't screen for fraud, you could expose your business to it. For one thing, you'll need to protect transactions that are out of scope for SCA, which could become a target for fraudsters once SCA comes into force."

In addition, a business's fraud rate will still be an important metric for acquirers and issuers, even when the business itself isn't liable for fraud. And the card scheme rules will still require businesses to keep their fraud rates below a certain level. "Use of transaction risk analysis and decisions about exemptions will depend on the overall standing of acquirers and issuers, and each merchant's fraud rate will affect the whole network," says Mark.

The fraud manager's role is evolving

There's little doubt that the role of the fraud manager is changing. Identifying and preventing fraud remain key objectives, but fraud teams are changing their approach, as Una explains: "To be effective, fraud managers realize they need to understand the risk faced by the organization as a whole."

That means measuring things like the global fraud loss rate across the company, order rejection rates and manual review rates, as well as the volume of fraudulent transactions that were successfully prevented. "Getting a grip on all of these numbers helps fraud management teams focus where they need to," says Una.

"Fraud managers are changing their focus: they're more concerned about the customer experience than they were before."

Mari-anne Bayliss, Cybersource

The fraud manager's role is evolving

(continued from previous page)

The fraud team's role is becoming broader. Rather than looking solely to reduce fraud and its cost, fraud managers are now:

- Addressing chargeback/dispute rates
- Reviewing authorization/conversion rates to fine-tune screening rules
- Aiming to control operational costs by moving to more automated and scalable solutions and reducing manual review
- Driving revenues by ensuring a better experience for genuine customers and by turning away fewer good orders

The trend generally is to consider fraud management as a higher-value, more strategic activity than before. "Fraud management is now being woven into the fabric of the business. The data that fraud management teams collect can help identify changes in customer behavior or purchasing patterns that can be used to help reformulate sales strategies," says Mark.

> "The change I've seen recently among MRC members is that they understand the importance of risk management to the bottom line, as well as its role in the overall strategic business planning for the company."
>
> Una Dillon, MRC

Top takeaways

To get ready for the future, businesses should:

1. Prepare and optimize for PSD2 SCA if they operate in the European Economic Area, UK or Gibraltar
2. Continue investing in their fraud teams as well as in automated solutions
3. Look to their fraud teams to help improve the customer experience
4. Consider using fraud management data to influence their strategic business planning

Bringing it all together

The experience of the pandemic shows that fraud strategies must be agile enough to help the business react quickly to new challenges and opportunities, and balance fraud management against revenue capture. Combining the right technology and data with human insight is critical to supporting those strategies.

And as merchants prepare for the future — including the changes that will come with PSD2 SCA — it seems likely that fraud teams will have an increasingly key role to play in helping develop business strategies that will drive revenues and growth.

"Merchants have always had to balance fraud prevention against payment optimization and the customer experience. The pandemic has highlighted just how dynamic that equation is, and how critical it is to take a smart approach. For me, that means combining technology with data and human insight to help teams adapt faster."

Andrew Naumann, Cybersource

How Cybersource can help

Our integrated suite of fraud management solutions helps merchants accept more good orders and give genuine customers a great experience — while keeping fraud under control.

At the heart of our solution suite is Decision Manager, our fraud management platform that combines machine learning (drawing on data from billions of transactions processed by Visa and Cybersource) with human insight to help you establish robust, flexible fraud strategies.

Decision Manager is complemented by Account Takeover Protection and other Cybersource and partner solutions, and by the expertise of our global team of Managed Risk Analysts.

Find out more at cybersource.com

Contact us

"Cybersource takes a holistic approach to help a merchant solve a challenge or take advantage of an opportunity. We have the breadth of tools and knowledge to help develop a solution to deliver the best results."

Mari-anne Bayliss, Cybersource

Flexible, creative solutions for everyday life

Cybersource helped kick start the eCommerce revolution in 1994 and haven't looked back since. Through global reach, modern capabilities, and commerce insights, we create flexible, creative commerce solutions for everyday life—experiences that delight customers and spur growth globally. All through the ease and simplicity of one digital platform to manage all payment types, fraud strategies, and more. Knowing we are part of Visa and their security-obsessed standards, you can trust that business is well taken care of—wherever it may go.

cybersource.com

cybersource
A Visa Solution