

eCommerce fraud explained

Your guide to understanding and managing online fraud



cybersource
A Visa Solution

Contents

Why this guide?	3
What does eCommerce fraud look like?	5
Why is eCommerce fraud so prevalent?	8
How does fraud management help?	12
How can the online payment process help combat fraud?	15
What are the top fraud management challenges?	17
What is the best way to manage fraud?	24
What tools should be part of your fraud management strategy?	30
What's the secret to optimal fraud management?	34
Cybersource offers fraud management solutions for every size company	37
Glossary of terms	40
Find out more	43

DISCLAIMER: The contents of this document 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. Cybersource and Visa are not responsible for your use of the information (including errors, omissions, inaccuracy, or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use.

Why this
guide?

What fraud
looks like

Why eCommerce
fraud is prevalent

Management
can help

Online
payments

Top fraud
challenges

Best way to
manage fraud

Tools for
your strategy

Optimal
management

Cybersource
can help

Glossary
of terms

Find out
more



Why this guide?

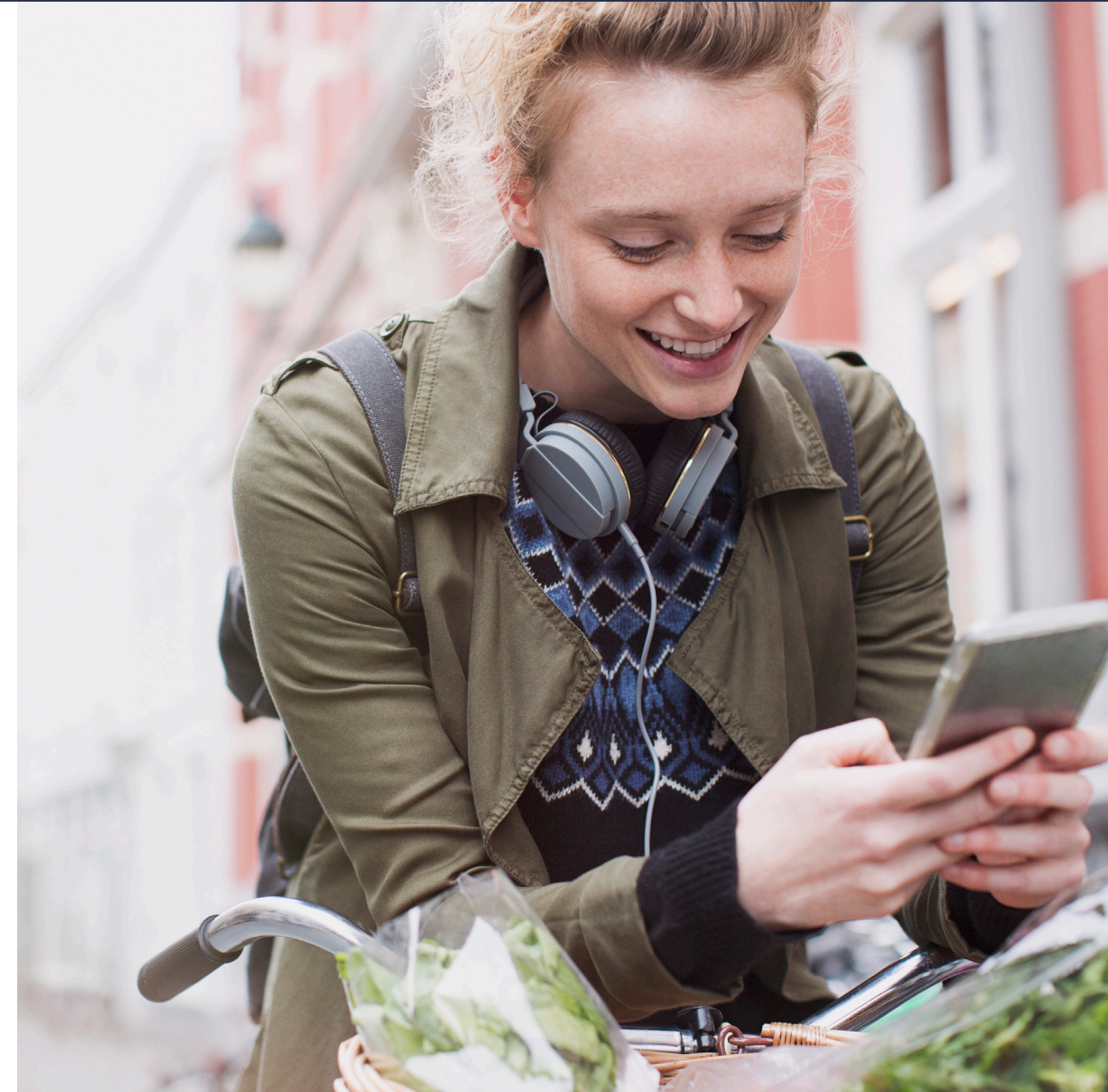
New insights on fraud management help get your business up to speed quickly

Many of the world's eCommerce giants turn to Cybersource to manage risk and reduce fraud. We help those businesses develop effective strategies and deploy an optimal mix of services to manage fraud effectively across channels and borders.

Your business might need new insights to expedite the move to Cybersource solutions from an in-house program, transition from other fraud services, or onboard a new employee in the anti-fraud department. Or you might be looking to develop a clear understanding of key concepts and strategies for eCommerce fraud management as you launch your business and get set up to accept digital payments.



This guide covers the basics for effective fraud management — to help you understand how to maximize revenue, minimize fraud loss and minimize operational costs.



What does eCommerce fraud look like?





From account takeovers to gray market sales, fraud takes many different ways, shapes and forms

eCommerce fraud has many faces. This illegal activity is carried out by an individual — or an organized crime group — through an online store. It results in unauthorized or fraudulent transactions, stolen merchandise, or wrongful requests for refunds. Read on to learn more about common types of eCommerce fraud.

Account takeover is growing

59%

of respondents surveyed for the Cybersource 2019 Global eCommerce Fraud Management Report indicated they anticipate account takeover attacks will increase in the next 12 months.¹

¹Cybersource, "Masters of Balance: What it takes to be a fraud management leader," 2019 Global eCommerce Fraud Management Report. By their nature, forward-looking statements are subject to risks, uncertainties, assumptions, and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements because of a variety of factors.

eCommerce fraud at a glance

Getting to know common types of eCommerce fraud

1

Account takeover

A fraudster uses stolen login credentials to gain control of someone else's account on an eCommerce site, on a bank site, or through a payment solution. The fraudster might change personal information or use payment details within the account to make purchases.

2

Buy online, pick up in-store

A fraudster uses stolen information to make a purchase online and then picks up the merchandise in a physical store before the retailer can detect the fraud.

3

Clean fraud

A fraudster uses a stolen credit card to make an online purchase, entering enough correct cardholder information for the transaction to look genuine and successfully pass the business's security checks.

4

Card testing

A fraudster uses an automated bot to conduct numerous small-value transactions with stolen credit card numbers. The goal of these tests is to determine which cards can be used for other, higher-value fraudulent transactions and which should be discarded.

5

First-person fraud

A customer buys an item using their own payment card, then claims that the purchase was unauthorized or the item did not arrive. The business reimburses the customer, who effectively gets the item free. (Also known as *friendly fraud*.)

6

Refund or return fraud

A fraudster buys merchandise online with stolen credentials, then goes to a physical store and requests a refund, most often receiving a store gift card due to the lack of a valid store receipt.

7

Reshipping fraud

A fraudster uses stolen payment details to buy goods. The fraudster then contacts the shipper and requests a redirect to a new address, or pays people — known as mules or freight forwarders — to act as delivery recipients. The mules reship the goods to the fraudster or another location for resale.

8

Gray market fraud

A fraudster buys goods with a stolen credit card and then resells them in unauthorized markets or geographies, or at a discount. (Also known as *reseller fraud*.)

9

Loyalty fraud

A fraudster gains unauthorized access to an account tied to a loyalty rewards program offered by a merchant.

[Why this guide?](#)

[What fraud looks like](#)

[Why eCommerce fraud is prevalent](#)

[Management can help](#)

[Online payments](#)

[Top fraud challenges](#)

[Best way to manage fraud](#)

[Tools for your strategy](#)

[Optimal management](#)

[Cybersource can help](#)

[Glossary of terms](#)

[Find out more](#)

A woman with dark hair pulled back, wearing a dark blazer, is shown in profile from the chest up, looking towards the left. She is in an office environment with blurred figures of other people in the background. The image is overlaid with a large blue semi-circle in the top left and a dark blue semi-circle in the bottom left.

Why is eCommerce fraud so prevalent?



Easy access to information and tighter in-store security have driven fraudsters online

The overall global spending on fraud management solutions for retail and eCommerce businesses is projected to reach EUR 9 billion by 2023.

Two main factors explain the high rate of eCommerce fraud:

Ease of acquiring information

- 1 It is cheap and easy for fraudsters to buy payment and identity information stolen during data breaches and hacks.²

Effective in-store fraud prevention

- 2 EMV (Europay, Mastercard, and Visa) technology embeds computer chips in credit cards to securely store cardholder data, known as “chip and pin” technology. As a result, criminals have moved more activity online.

Fraud shifts online

In-person, card-present fraud in the U.S. is down by

82%³

But online, card-not-present fraud in the U.S. is up by

33%⁴

² <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf>

³ Visa, chip card stats, November 27, 2018, https://usa.visa.com/visa-everywhere/blog.entry.html/2018/11/27/chip_technology_has-ulKX.html

⁴ Aite, “3-D Secure 2.0: Key Considerations for Card Issuers,” February 21, 2018, <https://www.aitegroup.com/report/3-d-secure-20-keyconsiderations-card-issuers>

By their nature, forward-looking statements are subject to risks, uncertainties, assumptions, and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements because of a variety of factors.



COVID-19 has changed the fraud landscape in unprecedented ways

As businesses begin to adapt to a “new normal” that includes rapid drops and surges in order volumes, new government policies, and depleted or displaced workforces, they may be unwittingly opening new doors and creating a more fertile environment for fraudsters.

Fraudsters are testing merchant’s accounts to see which ones have opened the door the widest. To keep your business and customers safe, you will need to take creative, proactive steps to understand and stay ahead of what has quickly become a nearly unrecognizable fraud landscape.

Trends

With the economy facing tough times, fraudsters know some businesses will likely be inclined to remove or adjust any perceived barriers to sales — giving them more opportunity to take advantage of weaknesses.

Manual fraud review teams could be understaffed and might move to accept/reject models or relax rules.

Card testing in particular has risen dramatically. In these attacks, fraudsters program botnets to run thousands of transactions on a merchant’s site to “test” the validity of card details. As a result, a number of merchants have seen authorization rates impacted.

Machine learning and AI models were not built with COVID-19 in mind, so you may see a number of false positives, which means you mistakenly reject genuine orders, during this period. You can expect these models to eventually recalibrate to COVID-related fraud trends. However this will take time, and it may be time you cannot afford to lose.

Takeaways

You should quickly evaluate new risk strategies without jeopardizing the payment experience your current customers enjoy. With Decision Manager Replay, you can test different “what-if” fraud strategies against your historical transaction data in real time. This lets you rapidly assess the impact of rules changes on your risk management strategy before putting them into production. As a result, you can more quickly identify the best rules changes to implement in your live environment.

If you need additional help to evaluate your fraud management strategy, **our Managed Risk Analysts are available to provide insights** and expertise during this time of crisis. They work across multiple industries and regions to stay in-tune with the latest tactics and approaches.

Rethink your approach to stay ahead of evolving fraud attacks

eCommerce continues to grow and evolve—and so does eCommerce fraud. To identify and safeguard against rapidly shifting fraudster strategies, it's more important than ever to adopt a modern fraud management system—one that uses advanced computer models and draws from constantly refreshed global transaction data.

Trends

eCommerce has grown rapidly since the mid 1990s. Today consumers use a variety of devices and payment methods to buy a wide array of products and services online.

eCommerce businesses are implementing omnichannel approaches. The goal is to deliver a seamless customer experience across eCommerce and traditional channels. Some businesses are enabling customers to browse for and buy items online that may be out of stock or not sold in a physical store. (Also known as *endless aisle*.)

Takeaways

eCommerce fraud is growing too. Fraudsters are continuously developing new practices and strategies to take advantage of the latest eCommerce sales channels and payment options.

The typical fraudster profile is also evolving. eCommerce fraud is no longer limited to individuals or small teams. Today fraud is an industry that involves national and global crime rings employing sophisticated techniques.⁵ So what do we mean by “today”? Cybersource has used national and international fraud crime rings in collateral for at least three years.⁶

⁵ US Federal Bureau of Investigation, “Transnational Organized Crime,” <https://www.fbi.gov/investigate/organized-crime>

⁶ Cybersource used a fraud evolution timeline showing national and international fraud crime rings.



A photograph of a man and a woman looking at a smartphone together. The man is on the right, wearing a dark blue hoodie and large headphones, holding the phone. The woman is on the left, wearing a red top, looking at the phone with a smile. The background is a bright, slightly blurred indoor setting. There are large blue and yellow circular graphic elements on the left side of the page.

How does fraud management help?

Fraud Management helps mitigate the risk of financial losses and damaged reputations



⁷ Cybersource May 2019 calculations based on eMarketer, Worldwide eCommerce and mCommerce, May 2019 (numbers have been rounded); and a GfK study commissioned by Cybersource, October 2018. By their nature, forward-looking statements are subject to risks, uncertainties, assumptions, and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements because of a variety of factors.



Keep chargebacks under control

An issuing bank reverses a payment, or performs a chargeback, to a business's account when a customer successfully disputes an item on their card statement with the card issuer. Fraud-related disputes fall into two categories.

- 1 **Third-party fraud:** a fraudster uses a cardholder's information to make an unauthorized purchase. The cardholder files a dispute with their issuing bank. It could take 30 days or longer for the cardholder to notice the fraudulent transaction when it appears on their statement.
- 2 **First-person fraud:** the cardholder disputes a legitimate charge to their credit card to avoid paying for the item. (Also known as friendly fraud.)

Payment networks such as Visa and Mastercard are strict about acceptable chargeback rates. Retailers with a chargeback rate that exceeds a card network's limit are placed on a chargeback watch list. Those retailers might also:

- ✓ **Incur higher processing fees** on orders, which would cut into profit margins
- ✓ **Lose the ability to fight chargebacks** until they bring their chargeback rate down
- ✓ **Be placed in a chargeback monitoring program** and required to pay further fees as the card association tries to help them reduce their chargeback rate

In contrast, optimizing chargeback rates is a mark of effective fraud management. The Cybersource 2019 Global eCommerce Fraud Management Report found that fraud management leaders have an average self-reported chargeback rate that is four times lower than others.⁸



When you optimize chargeback rates, you are helping minimize fraud losses without turning away good customers.

[Why this guide?](#)

[What fraud looks like](#)

[Why eCommerce fraud is prevalent](#)

[Management can help](#)

[Online payments](#)

[Top fraud challenges](#)

[Best way to manage fraud](#)

[Tools for your strategy](#)

[Optimal management](#)

[Cybersource can help](#)

[Glossary of terms](#)

[Find out more](#)

How can the online payment process help combat fraud?

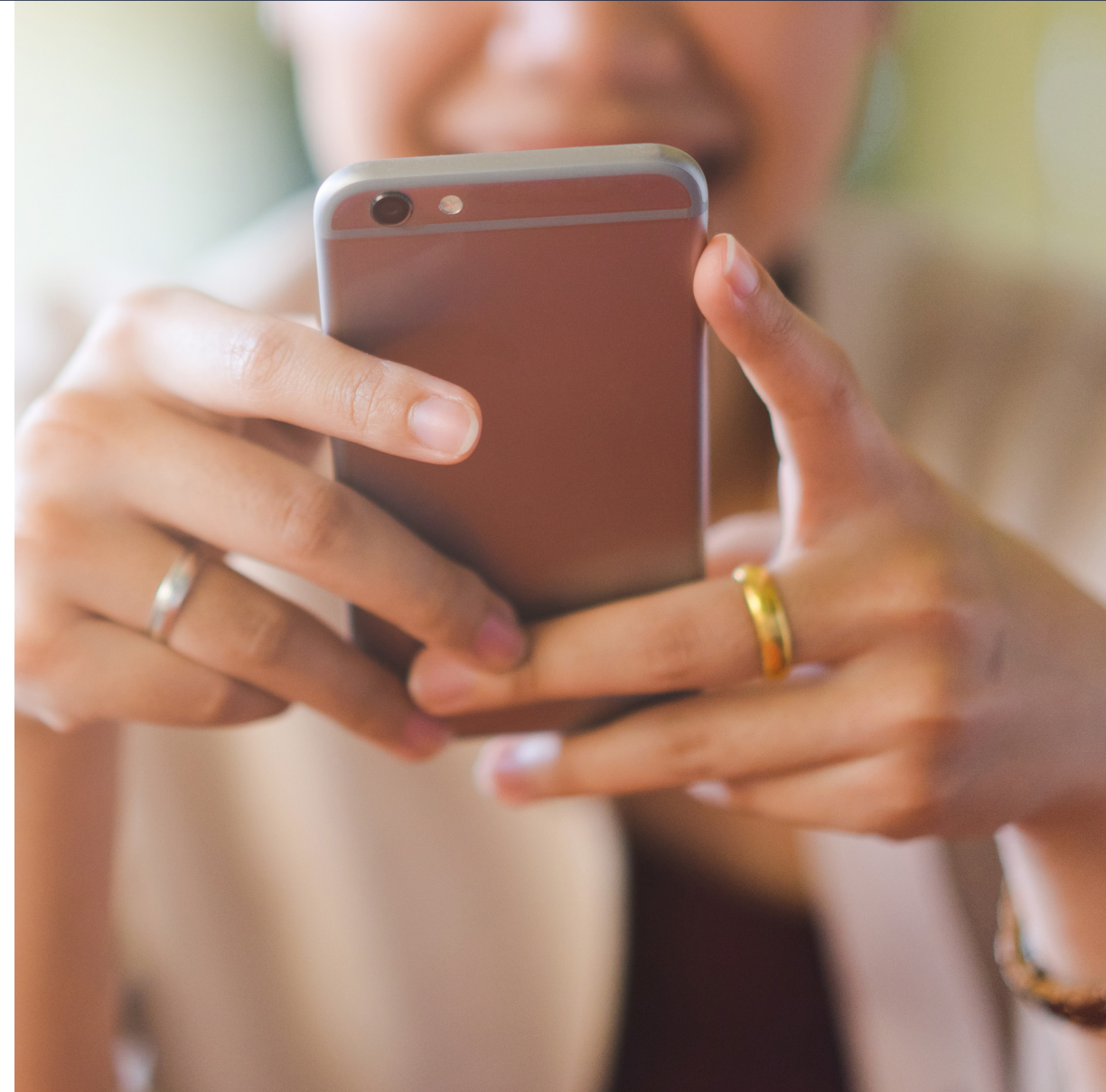


Understanding how online payments work helps plan your fraud management strategy

Online payments are multi-faceted processes that should work together to provide a frictionless customer experience while screening for fraudulent transactions.

For example:

- 1 **A customer clicks Buy Now**
- 2 **The business's payments gateway collects the transaction** and order information, and passes that information to its payment processor
- 3 **The payment processor checks with the customer's issuing bank to confirm:**
 - ✓ The card used is valid
 - ✓ Funds are available for the purchase
 - ✓ The transaction matches Address Verification Service (AVS) and Card Verification Value (CVV) responses
- 4 **With the issuing bank's confirmations, the payment processor will either:**
 - ✓ Put an authorization hold on the funds (so the retailer can review the order before funds are transferred), or
 - ✓ Schedule funds for transfer to the business's account at their acquiring bank



[Why this guide?](#)

[What fraud looks like](#)

[Why eCommerce fraud is prevalent](#)

[Management can help](#)

[Online payments](#)

[Top fraud challenges](#)

[Best way to manage fraud](#)

[Tools for your strategy](#)

[Optimal management](#)

[Cybersource can help](#)

[Glossary of terms](#)

[Find out more](#)



What are the top fraud management challenges?

A seamless customer experience, cross-channel sales, and regulatory compliance are top challenges⁹

For many businesses, the top fraud management challenges extend beyond stopping fraudsters. They should balance the goals of maximizing revenue, minimizing fraud loss and minimizing operational costs. At the same time, they want to create new, cross-channel experiences. And they should ensure they maintain compliance with emerging regulations.



⁹Cybersource, "Masters of Balance: What it takes to be a fraud management leader," 2019 Global eCommerce Fraud Management Report

Balance revenues, fraud loss, and operational costs

Effective fraud management can help you boost revenue through an outstanding customer experience, while you also combat fraud and enhance operational efficiency.

Maximize revenue: To deliver a seamless customer experience and keep your good customers happy, you should ensure smooth, fast and frictionless transactions. Your anti-fraud measures cannot slow transactions, mistakenly reject genuine orders (false positives), or otherwise inconvenience customers. Frustrating transactions could drive your customers to your competitors.

Minimize fraud loss: To detect fraudulent orders and prevent as many different types of fraud as possible, you should identify and respond to emerging fraud attacks. But that's not easy.

Minimize operational costs: No matter which fraud management solutions you adopt, you need to streamline and automate processes to control operational costs and keep fraud reviewer head count low.



Keeping pace with evolving types of fraud is often the top fraud management challenge identified by eCommerce businesses in 2019.¹⁰

¹⁰ Cybersource, "Masters of Balance: What it takes to be a fraud management leader," 2019 Global eCommerce Fraud Management Report

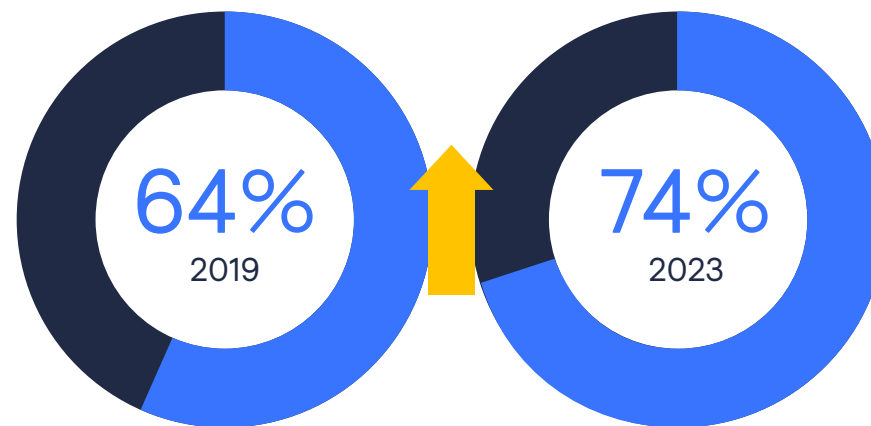




Adopt a cross-channel strategy

Focusing on genuine customer behavior can pay dividends in an increasingly omnichannel world, where consumers have lots of choices for how they shop. In addition to shopping in-person, over the phone and by surface mail, consumers increasingly use mobile apps from their smartphones and tablets as well as websites from their laptop and desktop PCs. In many cases, consumers use a combination of channels—for example, placing an order online and then picking up the product at a store.

Mobile payments are on the rise



By 2023, mobile is estimated to account for 74 percent of all eCommerce payments worldwide, up from 64 percent in 2019.¹¹

¹¹eMarketer, Worldwide eCommerce and mCommerce, May 2019 (numbers have been rounded). By their nature, forward-looking statements are subject to risks, uncertainties, assumptions, and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements because of a variety of factors.



Omnichannel takes priority

94%¹² of retailers say omni-channel fulfillment strategy is one of their company's top priorities.

¹² Forrester Data: Digital-Influenced Retail Sales Forecast, 2017 To 2022 (US)

Cross-channel fraud management helps you better understand genuine behavior

The fact that fraudsters will try to exploit different channels is reason enough to have a cross-channel strategy for fraud management. A cross-channel strategy also helps you understand genuine behavior. Customers who move between channels could look like fraudsters if you do not account for channel-related differences in purchasing behavior. This means you should have the ability to:

- 1 **Screen orders automatically** for fraud in channel-specific and device-specific ways
- 2 **Recognize genuine customers** (and orders) easily, and provide consumers with a seamless checkout experience in all channels

Comply with emerging regulations

As part of Payment Services Directive 2 (PSD2), new Regulatory Technical Standards have been created by the European Banking Authority. A key aspect of these security standards is the requirement for strong customer authentication (SCA). Currently, SCA is required only when both the acquirer and the issuer are located within the European Economic Area (EEA), UK and Gibraltar. PSD2 requires SCA to be applied to some electronic payments, including proximity, remote, and mobile payments within the EEA.

SCA requires consumers to verify their identity in two of three ways: presenting something they are (using biometrics); something only they have (a SIM card, preregistered mobile device, or token generator); and something they know (a PIN or password). Merchants should ensure they are ready to support SCA to prevent issuing banks from declining their transactions.

PSD2 SCA could impact any organization doing online business in the European Economic Area (EEA), UK and Gibraltar, as well as banks, fintechs, and other financial services firms that facilitate online payments.

The SCA mandate is complemented by limited exemptions that aim to support a frictionless payment experience—for example, when transaction risk is low, when transaction value is low and when merchants initiate the transaction.

Regulated issuers and acquirers are responsible for applying SCA and the exemptions that help achieve the right balance between customer convenience and fraud reduction.



To learn more about PSD2 SCA, visit www.Cybersource.com/en-gb/psd2-sca

Strong customer authentication (SCA) requires verification of the consumer's identity in at least two of three different ways



[Why this guide?](#)

[What fraud looks like](#)

[Why eCommerce fraud is prevalent](#)

[Management can help](#)

[Online payments](#)

[Top fraud challenges](#)

[Best way to manage fraud](#)


[Tools for your strategy](#)

[Optimal management](#)

[Cybersource can help](#)

[Glossary of terms](#)

[Find out more](#)



What is the best way to manage fraud?

A multi-layered approach helps you strike the right balance



A multi-layered approach — employing a range of tools and techniques — can help you accurately and efficiently distinguish between genuine orders and fraudulent ones.

No single tool can protect your organization against today's sophisticated eCommerce fraudsters. Point solutions, which focus on a single threat or capability, fail to protect against the full range of fraudulent activity. Moreover, a single-minded focus on minimizing direct losses makes it difficult to balance the goals of reducing fraud, delivering an outstanding customer experience, and expanding revenues.

Strategically layering a variety of fraud management tools that utilize multiple methods to detect fraud helps organizations defend themselves more effectively against a wider range of exploits targeting a growing number of sales channels. Businesses need to incorporate network-level protections as well as additional training to help teams better understand checkout flow best practices and how to detect and mitigate social engineering. Striking the right balance for your business also means integrating solutions that help increase approvals and minimize false positives in order to provide the best possible customer experience and maximize revenue.



Factor a broad range of tools and techniques into your layered approach



Counter constantly shifting fraud tactics with intelligent computer models

Artificial intelligence (AI) enables devices to reason and learn. **Machine learning** is an advanced form of AI that enables computer models to learn without requiring explicit programming.

Because intelligent computer models learn continuously through a variety of feedback mechanisms, they can deliver increasingly accurate results and generate fresh insights.

To work well within an automated fraud screening solution, a computer model needs to draw from large volumes of high-quality transaction data. A fraud screening solution should also provide an additional level of precision control, allowing you to combine computer analysis with rules based on human intelligence and parameters that make sense for your business.



As fraudsters change their tactics, intelligent computer models can learn, adapt and uncover emerging patterns to help prevent fraud.



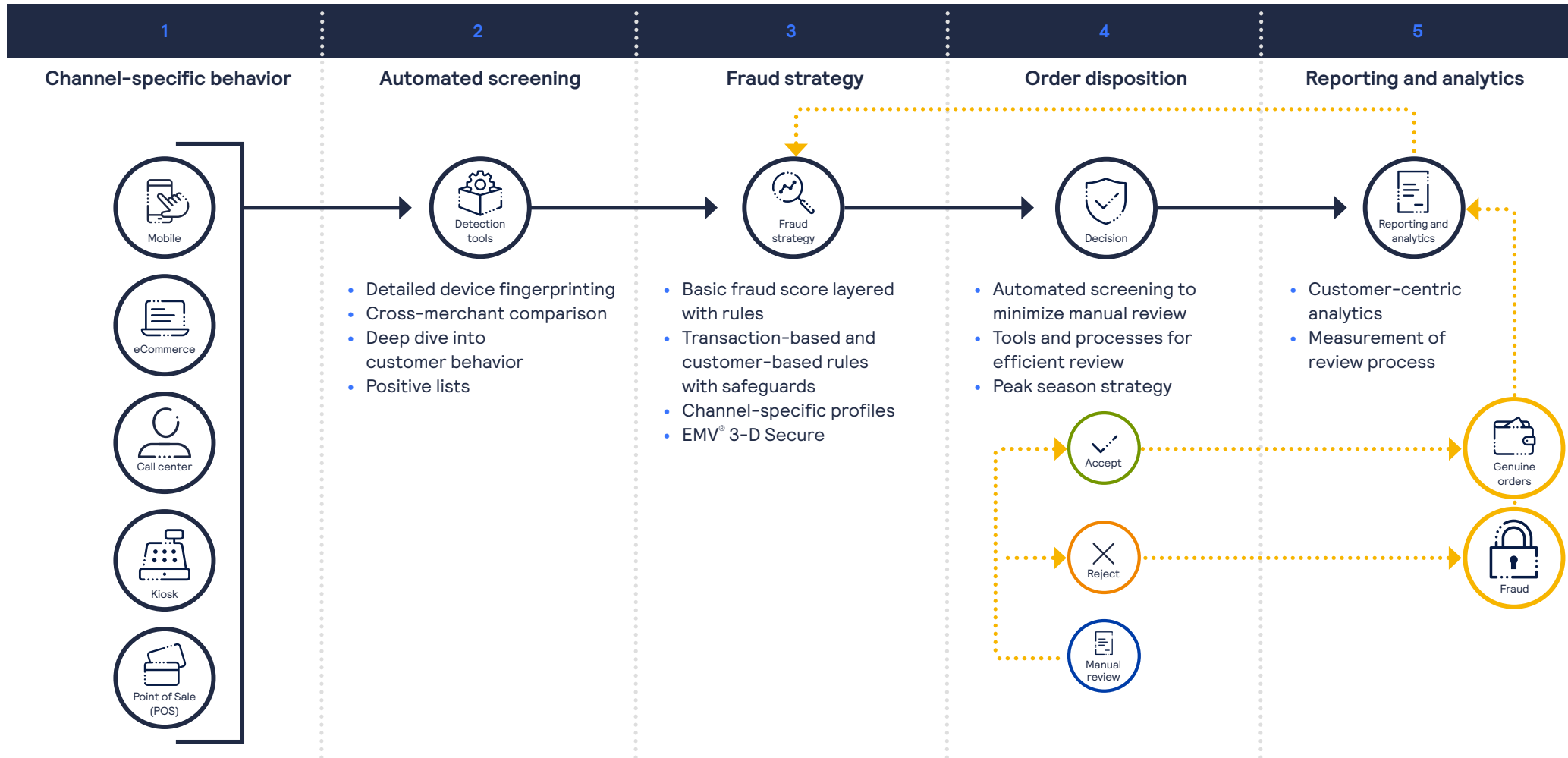


Determine the role of manual fraud screening

When you set up a new eCommerce operation, you may be able to manually check the small number of orders that come through initially. However, as order volumes ramp up, manual fraud screening can be time-consuming and costly. It might also harm the customer's experience if orders are held up because manual reviewers can't keep pace. When eCommerce business reaches this level, it's time to implement an automated fraud management system.

Manual transaction reviews should be reserved for situations when the accept-or-reject decision is unclear from your automated screening process. Reviewers can then apply a further range of techniques, and use their knowledge of your business and its customers to decide whether the order is genuine. The outcome of manual reviews can also act as a feedback loop, helping to continuously fine-tune the rules and computer models in your screening solution. Cybersource's machine learning model, in tandem with a flexible rules engine, represents a powerful combination that allows for swift and accurate responses to unique or emerging fraud trends.

Tailor your fraud management cycle to specific business requirements



[Why this guide?](#)

[What fraud looks like](#)

[Why eCommerce fraud is prevalent](#)

[Management can help](#)

[Online payments](#)

[Top fraud challenges](#)

[Best way to manage fraud](#)

[Tools for your strategy](#)

[Optimal management](#)

[Cybersource can help](#)

[Glossary of terms](#)

[Find out more](#)

A man with dark hair and a beard, wearing a dark brown sweater, is leaning over a wooden desk in a warehouse or office setting. He is focused on a laptop, with his hands on the keyboard. The background is filled with stacks of cardboard boxes, suggesting a logistics or e-commerce environment. The lighting is warm and natural, coming from a window on the right. A large yellow circle is partially visible on the left side of the image, overlapping a dark blue diagonal shape.

What tools should be part of your fraud management strategy?

Put screening tools with EMV® 3-D Secure and fraud-prediction analytics on your short list

Consider an optimal mix of solutions and services for your organization's fraud management strategy.

Fraud screening tools:

Validation services

- Postal address validation services
- Telephone number verification
- Email verification
- Geographic indicators and maps
- Biometric indicators
- Card Verification Value (CVV) validation
- Address Verification Service (AVS) validation
- Two-factor phone authentication
- EMV® 3-D Secure
- Credit history check
- Paid-for public record services

Your proprietary data and customer history

- Fraud scoring models (company-specific)
- Customer website behavior and pattern analysis
- Customer order history
- Negative lists (in-house lists)
- Positive lists (in-house lists)
- Order velocity monitoring
- Proxy detection

Multi-merchant data and purchase history

- Credit card fraud alert services from third-party aggregators
- Shared negative lists (also known as hotlists)
- Multi-merchant purchase velocity and identity morphing models

Purchase device tracking

- Geolocation—laptop, desktop PC, mobile device, and tablet
- Device fingerprinting
- Web browser IP address





Protect against fraudulent chargebacks

EMV® 3-D Secure helps thwart fraud-related chargebacks. This technology enables real-time authentication of the payer during an online transaction.

To avoid introducing unnecessary friction during the checkout process, employ a rules-based approach that lets you decide when to request additional authentication. You can preserve the customer experience and reduce the likelihood of checkout abandonment while continuing to benefit from the liability shift by sending only the most risky transactions through 3-D Secure. This is only applicable in the regions where SCA is not mandated.



When transactions are verified by 3-D Secure, card schemes may impose regulations on the issuer that move the financial liability for fraudulent transactions to the issuer. This is referred to as liability shift and it is important for merchants to understand the regulations in place by card scheme in their location.

Cybersource rules-based 3-D Secure preserves a frictionless customer experience



Order checkout

- Only selected orders are challenged using pre-configured authentication rules

Separate order flows based on risk

- Intelligent rules route high-risk customers to a challenge

Business outcomes

- Less risk of lost sales due to transaction friction
- Reduction in chargebacks
- Potential interchange savings
- Liability shift
- Reduced manual review

*Illustrative example only.

This applies in markets not regulated under PSD2 SCA or any other customer authentication directive.

[Why this guide?](#)

[What fraud looks like](#)

[Why eCommerce fraud is prevalent](#)

[Management can help](#)

[Online payments](#)

[Top fraud challenges](#)

[Best way to manage fraud](#)

[Tools for your strategy](#)

[Optimal management](#)

[Cybersource can help](#)

[Glossary of terms](#)

[Find out more](#)



What's the secret to optimal fraud management?

Tap into Cybersource's fraud-prediction technology

A holistic, multi-layered fraud management strategy capitalizes on sophisticated machine learning and artificial intelligence to balance effective fraud prevention, a seamless customer experience, and operational efficiency. Our experts can help you implement Cybersource fraud management solutions to help increase decision-making accuracy, capture more revenue and benefit from deep domain expertise.

Increase accuracy

Cybersource generates risk scores using the only machine learning models built and maintained by data scientists from both Visa and Cybersource, tapping into decades of experience. These models draw insights from billions of transactions processed around the world—and each transaction can have up to hundreds of data fields such as device fingerprint, IP address, geolocation and more. Given such large volumes of rich data that is updated in real time, Cybersource's unparalleled machine learning models enable businesses to improve their accuracy and speed in detecting new fraud patterns while reducing false positives.

Capture more revenue

Optimizing authorizations to capture more revenue is the next key step in a balanced fraud management strategy. Issuers' eCommerce authorization rates still lag well behind brick-and-mortar authorization rates. Cybersource is working to close this authorization gap by changing the way that transactions are processed. Our Revenue Capture initiative is shifting the way businesses and issuers interact by providing greater visibility into decision making in order to help issuers make more informed authorization decisions.

[Read our Revenue Capture whitepaper to learn more.](#)



Enterprise-grade fraud-prediction technology analyzes each transaction's probability of risk. Cybersource offers the only fraud management solution with machine learning models built on the combined decades of experience that Visa and Cybersource have worldwide.

Cybersource fraud management solutions are built upon deep fraud domain expertise



20+ years

of experience in developing **machine learning models** and rules-based fraud management software



800+ years¹³

of combined **expertise across dozens of verticals and geographies**, including more than 65 analysts on five continents available for consulting services



24/7

add-on services available worldwide, including fraud screeners to help **manage peak seasons** or handle overflow manual reviews



Hundreds of millions¹³

of dollars in ongoing **investment in fraud management software**, hardware and personnel

¹³ As of 08/01/2020

[Why this guide?](#)

[What fraud looks like](#)

[Why eCommerce fraud is prevalent](#)

[Management can help](#)

[Online payments](#)

[Top fraud challenges](#)

[Best way to manage fraud](#)

[Tools for your strategy](#)

[Optimal management](#)

[Cybersource can help](#)

[Glossary of terms](#)

[Find out more](#)



Cybersource offers fraud management solutions for every size company

A full range of world-class fraud solutions and services to fit your needs

Small and mid-sized businesses

Fraud Management Essentials

Fraud Management Essentials is the only payments gateway fraud management solution with enterprise-grade Cybersource fraud-prediction technology and simple, pre-configured fraud settings built in. It automatically checks for risky transactions and enables you to set transaction filters for the way you do business.

- Detect fraud with reliable screening and powerful machine learning-based computer modelings.
- Accelerate setup with built-in fraud rules and pre-configured settings.
- Reduce chargeback and declined authorization costs of card testing and common fraud attacks.
- Make informed decisions with a user-friendly dashboard.
- Reduce fraud without adding friction to checkouts with customer-friendly fraud protection.

Get the best of both worlds — an out of the box fraud solution with access to fraud detection technology.

Account Takeover Protection

Shield customer accounts against fraudulent use of payment data by actively monitoring new account creation and account usage according to your rules.

Enterprise businesses

Decision Manager

Streamline your fraud management operations by taking advantage of powerful detection tests, screening models, case management capabilities and real-time reporting. Cybersource Decision Manager uses sophisticated machine learning models, in tandem with a flexible rules engine, to deliver swift and accurate responses to unique and emerging fraud trends.

- **Rules Suggestion Engine:** Apply Decision Manager's advanced machine learning to your historical transaction data to automatically suggest new rules without human bias.
- **Decision Manager Replay:** Reduce testing time from months to a matter of minutes. Test different what-if fraud strategies against your historical transaction data to assess the impact of fraud strategy changes.

Managed Risk Services

Hire the expert team of Cybersource risk analyst consultants available across five continents to optimize Decision Manager results. Scale your operations with 24/7 availability of add-on screening management resources.

Account Takeover Protection

Shield customer accounts against fraudulent use of payment data by actively monitoring new account creation and account usage according to your rules.



Additional fraud and risk management solutions

[Delivery Address Verification](#)

Verify typed address and correct invalid city, state, ZIP code/postcode combinations for orders originating in over 200 countries and territories.

[Fraud Alert](#)

Receive consumer-confirmed fraud notifications in near real time so you can stop shipments, save fulfillment costs and prevent chargebacks.

[Loyalty Fraud Management](#)

Implement a comprehensive fraud management solution that analyzes access behaviors, monitors suspicious account changes and analyzes checkout purchases using hundreds of fraud detection tests with Cybersource's Account Takeover Protection.

[EMV® 3-D Secure](#)

Specify rules for which transactions go through the 3-D Secure process and which do not, to improve the customer checkout experience.

[Why this guide?](#)

[What fraud looks like](#)

[Why eCommerce fraud is prevalent](#)

[Management can help](#)

[Online payments](#)

[Top fraud challenges](#)

[Best way to manage fraud](#)

[Tools for your strategy](#)

[Optimal management](#)

[Cybersource can help](#)

[Glossary of terms](#)

[Find out more](#)

A woman with dark, curly hair, wearing a bright yellow sweater, is looking down at a light blue tablet computer. She is holding a credit card in her right hand. The background is a blurred indoor setting with warm lighting and wooden walls. There are two large circular graphic elements: a blue one in the top left and a dark blue one in the bottom left.

Glossary of terms

Get going with basic concepts and terms for eCommerce fraud management

Account takeover fraud: The use of stolen login credentials to gain control of an account and commit fraud.

Address Verification Service (AVS): A tool that verifies the address and ZIP code/postcode that the customer provides during the order process. It compares the numerical portion of the address with card information on file at the customer's issuing bank.

Artificial intelligence (AI): Technology performing functions that traditionally require human intelligence, such as reasoning and learning.

Card Verification Value (CVV): A three-digit or four-digit security code on a payment card, which the customer provides during the purchase process. The bank checks this code as a way to verify that the card is present at the time of purchase.

Chargeback: The process whereby an issuing bank reverses a payment to a business's account, after a customer successfully disputes an item on their card statement.

Clean fraud: The fraudulent use of a stolen credit card and cardholder information to make an online purchase look legitimate.

eCommerce: Buying or selling products online using web, mobile, or other technologies.

EMV (Europay, Mastercard, and Visa) technology: Computer chips embedded in credit cards to securely store cardholder data, helping to prevent fraudulent in-store purchases. (Also known as chip-and-PIN technology.)

Endless aisle: The experience enabling in-store customers to easily browse for and order a broad range of products online that may be out of stock or not sold in-store, and have them shipped to the store, home, or other location.

First-person fraud: The cardholder's fraudulent claim that a purchase was unauthorized or the item did not arrive. The customer is reimbursed but keeps the item. (Also known as friendly fraud.)

Fraud screening: A predictive analytics approach that assesses risk by drawing upon both current and historical data.

Gray market fraud: The purchase of goods with a stolen credit card and sale of those goods in unauthorized markets or geographies, or at a discount. (Also known as reseller fraud.)

Liability shift: When a transaction verified by EMV[®] 3-D Secure, authentication turns out to be fraudulent, the card issuer assumes financial liability (except for recurring transactions).

Machine learning: An advanced form of artificial intelligence that enables computer models to learn without requiring explicit programming.

Manual review: The process of having a human review an order when the decision to accept or reject the order is not clear from an automated screening process.

Negative list: A list or database including credit card details, customer names, email addresses, physical addresses and sometimes entire countries or regions that have been identified as fraudulent or risky. (Also known as hotlist.)

Omnichannel: The business strategy to deliver seamless customer experiences across eCommerce and traditional sales channels.

Payer authentication: A technology that enables real-time authentication of the payer during an online transaction. (Also known as EMV[®] 3-D Secure.)

Payment Services Directive 2 (PSD2): PSD2 is the second Payment Services Directive, designed by the countries of the European Union. It was implemented on January 13, 2018. It may revolutionize the payments industry, affecting everything from the way we pay online, to what information we see when making a payment.

Glossary continued

Positive list: A list or database of known no-risk and low-risk customers or cards whose orders are instantly approved, without undergoing a review process.

Refund or return fraud: The process of purchasing merchandise online using stolen credentials, and then going to a physical store to receive a refund or a gift card.

Reshipping fraud: The practice of using stolen payment details to buy goods, and then either contacting the shipping company to redirect delivery to a new address, or paying people (known as mules or freight forwarders) to receive the goods and reship them to a different location for resale.

Rules system: A solution that uses an if-then approach to trigger fraud management functions.

Statistical scoring model: The evaluation of transactions based on known customer profile information, such as order history, purchase velocity, device tracking, and previous fraud.

Strong customer authentication (SCA):

As part of Payment Services Directive 2 (PSD2), new Regulatory Technical Standards for authentication have been created by the European Banking Authority. SCA requires consumers to verify their identity in two of three ways: presenting something they are (using biometrics); something only they have (a credit card, mobile device, or token generator); and something they know (a PIN or password).

Suspicious activity monitoring: A solution designed to detect activities that might indicate account takeover fraud.

Third-party fraud: The fraudulent use of a cardholder's information to make an unauthorized purchase.

EMV® 3-D Secure: A technology that enables real-time authentication of the payer during an online transaction. (Also known as payer authentication.)



Find out more

Discover how Cybersource can help you stop fraud, streamline the customer experience and control costs

eCommerce fraud will continue to grow and evolve. By moving forward with a holistic, multi-layered approach to fraud management, your organization can maximize fraud prevention and enhance operational efficiency. All while delivering an exceptional customer experience and helping to grow your eCommerce revenues.

Dive deeper

Explore the full range of Cybersource fraud management solutions: www.cybersource.com/fraud. Learn how to become a “Master of Balance” by tapping best practices from eCommerce leaders around the world. And download our free global fraud report: www.cybersource.com/fraudreport.

Contact us

For more information, visit: www.cybersource.com

cybersource
A Visa Solution

© 2020 Cybersource Corporation. All rights reserved.

All brand names and logos are the property of their respective owners, are used for identification purposes only, and do not imply product endorsement or affiliation with Visa.

DISCLAIMER: Case studies, 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. You should consult with your legal counsel to determine what laws and regulations may apply to your circumstances. The actual costs, savings, and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties, and assumptions that are difficult to predict or quantify. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracies, or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party’s intellectual property rights. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental, or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

© 2020 Cybersource Corporation. All rights reserved | www.cybersource.com

Updated July 2020 | 43