The Good, The Bad and The ID: Identifying Fraud & Securing Customer Loyalty

Find out how to drive loyalty, save time and boost revenue by identifying good customers – and stopping the bad – at your point of sale.

Overview

Global payment fraud is on the rise and projected to cost merchants over **£38 billion by 2027**[1], fuelled by the relentless swell of online fraud attacks growing in both size and sophistication.

The result? Merchants are increasingly left walking a tightrope of balancing costs and customers with risk and revenue.

From rising fraud prevention costs to the cost of fraud losses and compliance, today's businesses must also consider the cost of damaging customer loyalty and potential lost sales due to poorly policed attacks, when assessing their fraud prevention strategy.

Get it wrong, and companies, their customers and their bottom line all suffer. But with the right approach, merchants can secure a sales-savvy future – one where good customers are protected, the bad are detected, and costs are corrected.

Merchants lose £1.70 for every 71p taken by a fraudster.[2]

Overview

This eBook has been designed to help eCommerce, Risk and Fraud leaders, and business owners navigate the ever-changing face of online fraud protection, with a unique focus on:

Identifying good and bad customers

What 'good' and 'bad' look like at point of sale; how an effective process unveils stronger retention and revenue opportunities – and just how damaging bad customers really are.

Customer loyalty

Why good customers are loyal customers – and why a poor ID and/or Fraud process can impact more than just your reputation.

Saving time and building efficiencies

How comprehensive partnerships and ease of integration with the right platform drives better protection, quicker support and faster response times.

Good Customers vs. Bad Customers: Realising the Relationship

Good Customers vs. Bad Customers: Realising the Relationship

Customers want effortless experiences with absolute security; a panacea companies are struggling to meet. As the proliferation of online payments continues at breakneck speed, unveiling new – and increasingly more sophisticated – opportunities for fraudulent activity at point of sale (POS).

Merchants have been left feeling the strain of expectation on digital transactions and customer experience like never before.

Faster customer journeys. More secure payment transactions. Enhanced customer experiences. All against a backdrop of fraud and payment ID processes expected to keep pace with the new face of digital demand.

"To a business, the loss of a good customer is as bad as fraud...that customer could be with them for 20-30 years and be a very profitable individual."

Equifax's 'Fraud Prevention & Customer Experience'[3]

For digital merchants, it's a trifecta challenge:

- ✓ Mitigate payment fraud,
- ✓ Deliver effortless customer experiences,
- ✓ Enable revenue growth.

To do so, merchants must be better equipped to identify, engage and service their good customers at POS – while eliminating the bad. Knowing the difference is business critical.

Good vs. Bad customers: Understanding Personas

Personas help fraud prevention systems – through the use of AI and machine learning – identify expected 'normal' behaviour at point of sale, letting legitimate customers convert and flagging potentially fraudulent activity.

Amongst the hundreds of persona variables robust prevention algorithms deploy to assess purchasers in real-time during attempted transactions, common components of identifying good customers from bad include:

- ✓ User profile and login attempts
- ✓ Number of credit cards & email addresses linked to the persona
- ✓ Actual location and other device identification characteristics
- ✓ Mobile and/or browser-based characteristics
- ✓ Payer identification & authentication
- ✓ Comparing user location and shipping destination
- ✓ Assessing large transaction amounts
- ✓ Previous purchasing history

While each merchant's detection parameters will remain unique to their own risk and persona profiles, defining the subsequent action taken is crucial.

Get it right, and good customers prevail through a positive purchasing experience, while merchants secure trusted revenue with diminished risk – safe from the damage of potentially fraudulent actors.

Get it wrong – either by letting bad customers through or rejecting good customers – and the ramifications remain the same: a costly loss of revenue.

So, how do merchants strike the balance of a rigorous payment fraud process with seamless experience, to protect good customers and boost revenue?

The Power of Process: Why Good Customers Mean Better Business

An effective payment fraud prevention solution has its good customers at the very core of its process.

Why? Because it's not just about protecting revenue – it's about protecting loyalty. Merchants on the frontline are continually assessing the balance of supporting good customer experience against bad customer intentions to maximise revenue and elevate customer loyalty.

10-15%

of eCommerce sales are fraudulent in the UK. This is double the rate pre-covid.[4]

Of course, mitigating fraudulent activity from bad actors is priority number one, but an effective payment strategy must do so without stifling the experience and purchasing freedom of a merchant's good customers.

> **Without careful consideration, overbearing processes can damage customer loyalty and potentially lose good customer revenue, forever.**

Ultimately, the quicker merchants identify and expedite good customers, the more revenue they generate. Here's what to consider when assessing how bad processes impact good customers – and why good processes positively impact a merchant's top line...

The Payment Process Perspective

Best

Good customers, good process

- ✓ Balanced fraud persona detection
- ✓ Supervised & unsupervised AI and machine learning, with historical & real-time data
- ✓ Delivers accurate predictions based on behaviours and trends
- ✓ Combines with the merchant's customer experience strategy
- ✓ Continually updated, bespoke company policies swiftly define approve/review/decline outcomes
- ✓ Bad customers are identified, rejected and fed back into the algorithm
- ✓ Good customers are approved at speed and continue the transaction in line with wider customer experience strategy
- ✓ A seamless customer experience with loyalty and revenue opportunities prevails

Bad customers, good process

- ✓ Targeted fraud persona detection
- ✓ Supervised & unsupervised AI and machine learning, with historical and real-time data
- ✓ Delivers accurate predictions based on behaviours and trends
- ✓ Bespoke company policies define approve/review/decline outcomes
- ✓ Bad customers are identified, rejected and data captured for future use
- ✓ A trusted, secure process prevails to diminish fraud risk and protect good customers

Good customers, bad process

- ✓ Unconfigured fraud persona detection
- ✓ Unsupervised machine learning, from generic marketplace data
- ✓ Delivers overbearing predictions based on fraudulent behaviours and trends
- ✓ Rigid, unchecked plug-and-play policies define approve or decline outcomes
- ✓ Bad customers are identified, rejected and data stored for compliance and audit checks
- ✓ Good customers are mis-identified, rejected and a receive negative payment experience
- ✓ Potential bad actors are identified at the cost of lost sales and loyalty from good

Bad customers, bad process

- ✓ Outdated fraud persona detection based on unsupervised machine learning and manual reviews
- ✓ Delivers loose predictions based on generic purchasing behaviours and trends
- ✓ Poorly-defined company policies govern majority approved outcomes
- ✓ Bad customers remain unidentified and free to complete fraudulent transactions
- ✓ Good customers complete honest transactions at the cost of poor customer experience, potential product delays and impacted customer lifetime value

Worst

Customer Loyalty & Saving Time

Customer Loyalty & Saving Time: Reaping the Reward

As the online payment landscape continues to evolve the customer experience, behind the digital scenes merchants are contending with the equally-evolving sophistication of fraud threat vectors, and the time taken to manage them efficiently.

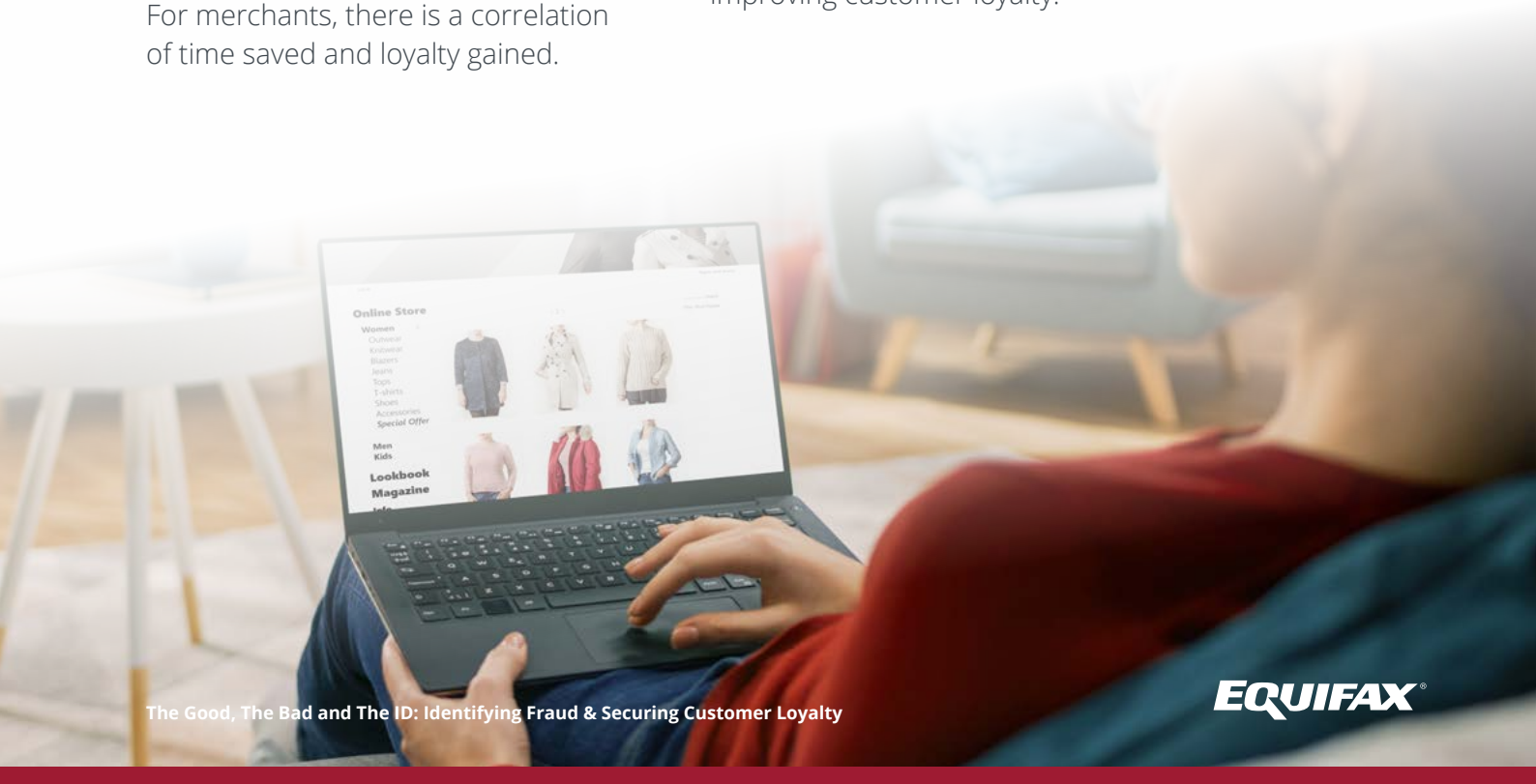
£1.3bn

...UK victims lost £1.3bn in 2021 amid a surge in online fraud.[5]

With it, the amount of human-power and time committed to manually reviewing and handling fraud-related queries – both legitimate and otherwise – is increasing significantly; directing valuable time away from revenue-driving and customer loyalty-building activities.

For merchants, there is a correlation of time saved and loyalty gained.

From chargebacks to account takeovers, having a controlled, AI-powered payment fraud prevention solution not only increases the speed and efficiency of resolution – it reduces time otherwise used in manual review, freeing up teams to focus on pursuing innovation and improving customer loyalty.



EQUIFAX®

Here are five ways merchants can save time and increase customer loyalty with their payment fraud process:

1. **Automate review handling where possible:** Doing so will reduce the amount of manual review teams are tasked with, while scaling process efficiencies

2. **Build AI & Machine Learning into the review process:** This will increase review accuracy and decision speeds, helping create a more seamless customer experience

3. **Recognise existing customers tied to previous purchases:** This creates an opportunity to deliver secure, personalised experiences that drive customer loyalty

4. **Implement a dispute monitoring programme:** Help cardholders recognise disputed transactions in real-time, reducing communication friction and increasing customer trust

5. **Ensure partner compliance:** Partner with providers who can ensure, manage and report on compliance intelligence, easily digestible for customer peace of mind

Of course, automation isn't about replacing fraud teams. It's about streamlining process efficiencies that increase the speed and accuracy of tasks – unshackling teams from the constraints of manual intervention and augmenting their strategic effectiveness.

It also enables scalability of process, ensuring standards and quality of outcome remain during sudden (and often seasonal) fluctuations in transaction volumes; fluctuations that typically create riskier transaction approvals or grind operations to a halt with growing backlogs, when deploying manual review-heavy processes.

Merchants able to combine automation with AI & Machine Learning to reduce human error and recalibrate existing team resource within their payment fraud process, not only benefit from the above – they reap the reward of deepened customer loyalty, including:

- ✓ More time handling and reviewing high-touch customer cases
- ✓ Supporting strategic value-add areas of the customer journey
- ✓ Proactively working on fraud detection innovations
- ✓ Less time spent in fraud & chargeback manual reviews, more time supporting customers
- ✓ Enabling personalised customer experiences
- ✓ Increasing speed and security of customer transactions

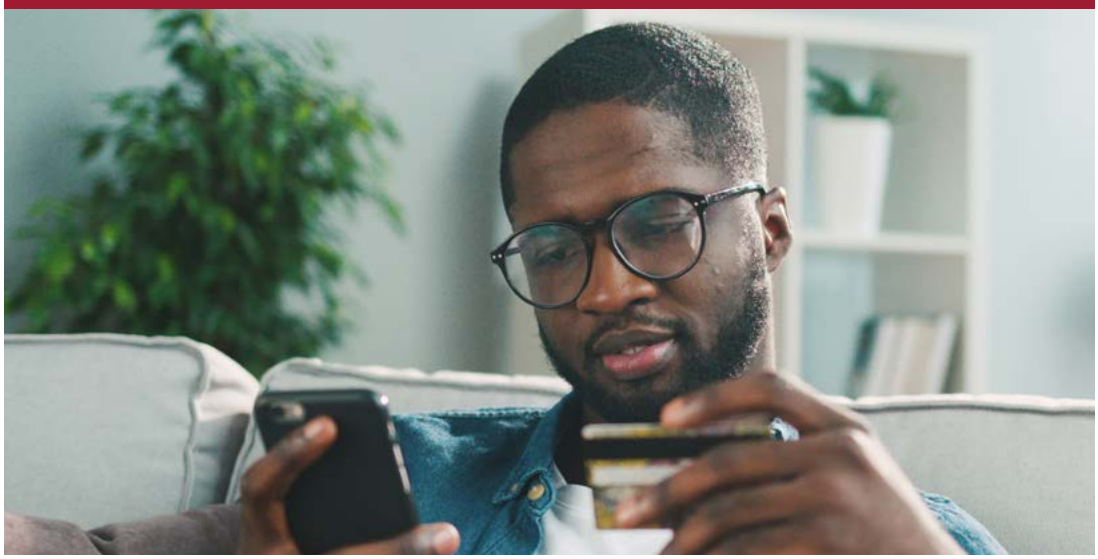
While time is always of the essence, accurate and efficient decision-making must remain. Payment fraud processes that balance speed with precision will identify and respond to fraudulent actors without compromising the customer's experience or trust in the merchant.

Fraud losses on UK-issued cards totalled

£524.5m in 2021[6]

Merchants with third-party providers who are able to offer protection and support around this when dealing with the likes of chargebacks and account takeovers, will heighten their ability to react quicker, resolve faster and deliver a superior experience that drives customer loyalty with protection at its core.

And what works for the customer, works for the merchant, too. With more time and better customer loyalty in hand, merchants and their fraud teams can shift their focus from reactive review handling to proactive revenue generation support – unveiling new innovations and best practices that feed back into the customer journey and extend lifetime value.



Switching Providers: Ensuring Ease of Integration & Compliance

Switching Providers: Ensuring Ease of Integration & Compliance

For most merchants, restructuring payment fraud processes is ill-afforded downtime. Like switching the engine of a moving car, any significant repositioning – whether to process, platform or provider – must happen in motion to avoid impacting performance and prevention capabilities.

And when it comes to switching providers, the typical sentiment is even clearer: complex, costly and time-consuming.

For merchants already challenged in matching the relentless fluidity of fraud attacks, decisions to change platform and provider are often driven by a necessity to move, instead of a desire to enhance.

And it's easy to understand why. From legacy pricing models with limited support – to long-winded integration and onboarding processes – switching providers can cost fraud teams time, money and exposure to risk that ripples out long past the initial decision.

Choose the right provider, however, and the exact opposite prevails.

Here's what merchants should expect when exploring a potential provider switch:

- ✓ Proven speed & ease of integration
- ✓ Customisable controls
- ✓ Transparent pricing
- ✓ Dedicated and ongoing support
- ✓ AI & Machine Learning capabilities
- ✓ Advanced Data Analytics
- ✓ Easily measurable ROI

Providers committed to delivering industry-leading solutions with speed and ease of integration at their core, unlock new efficiencies for merchants, their fraud teams – and their customers – including:

Less time integrating, more time implementing

Enhanced data visibility to drive quicker decisions

Realigned resource towards revenue-driving activities

Significantly reduced manual reviews & chargebacks

Elevated customer experience and a seamless payment journey

Proactive and trusted compliance best practice

While speed and ease of integration should be a priority for any potential provider switch, compliance must remain paramount throughout – both internally for the merchant and externally with the customer – in providing clear intelligence back to banks and consumers.

> **Customer-side, proactive compliance builds trust; trust that folds into deepened customer loyalty and an increase in more 'good' customers over time.**

Conversely, the impact of poor compliance hurts more than just customer loyalty for merchants – provoking Financial Conduct Authority (FCA) action and potential blacklisting that translates into higher interest fees and lost business.

By combining the right provider with robust processes and clear fraud prevention objectives, merchants can harness new partnerships at speed that build operational efficiency, reduce chargebacks and takeovers – and champion revenue generation opportunities.

Key Takeaways

Key Takeaways

Today's merchants need to keep pace with tomorrow's fraud threats.

Manual and time-consuming payment fraud processes reduce the efficiency and speed of teams to identify and engage proactively with 'good' customers, focus strategically on customer loyalty and unlock new revenue and profit-generating opportunities.

1. **Know how to identify good and bad customers:**
   Understand the behaviours and personas at play and how your POS, review and payment processes engage with each
2. **Automate manual reviews:**
   Remove time spent handling chargebacks and account takeovers, and realign resource towards customer and revenue objectives
3. **Champion customer loyalty:**
   Realign internal resource to elevate processes that recognise and reward good customers and increase their lifetime value
4. **Reduce costs:**
   Quicker response times and more accurate outcomes through automation, AI & Machine Learning drive operational efficiencies and protect budgets
5. **Secure fraud prevention providers with ease of integration:**
   Leverage industry-leading solutions that save time, money and customers

Elevate your fraud payment strategy and harness the power of true customer loyalty.

Find out how Kount is helping the UK's leading online merchants keep their transactions trusted and payments protected with customer loyalty at its core. Get in touch today.

Contact us

References

1. FinancesOnline, '57 Crucial eCommerce Fraud statistics for 2022: Types, Cost & Protection Data'
2. Expert Market, 'Chargeback Fraud Statistics 2022: Everything You Need to Know About Chargeback Fraud'
3. Equifax, 'Fraud Prevention and Customer Experience'
4. Opayo, 'Ecommerce Fraud Trends to look out for in 2021'
5. The Guardian, 'UK victims lost £3.1bn in 2021 amid surge in online fraud, new data shows'
6. UK Finance, 'Annual Fraud Report: The Definitive Overview of Payment Industry Fraud in 2021'