WHEN THE ECONOMY TURNS DOWN, FRAUD GOES UP

identiq

80%

of Certified Fraud Examiners say fraud levels rise in times of economic distress.

We hope we aren't heading there - but fraud fighters need to be prepared in case it happens. And preparation needs to start now.

At the same time, fraud prevention teams are under pressure. Prior to Covid-19, **45%** of organizations rated their fraud prevention effectiveness as high or very high. A year later, only **34%** rated themselves that way.

FRAUD FIGHTERS NEED TO GET READY

What do you need to prepare for?
Here are some likely areas to consider.

FRIENDLY FRAUD

Friendly fraud first became a serious problem in 2008-9 - during the economic crisis.

#1 CONCERN across industries and geographies

In 2021, for the first time, the annual MRC global payments and fraud survey found that friendly fraud has become the **No. 1** concern for merchants across industries and geographies.

In 2022, the survey found that merchants believe an astonishing **16%** of fraudulent disputes should be attributed to first-party misuse.

And a 2022 NRF study found that **more than two-thirds (68%)** of those earning less than $50,000 a year are having to borrow money, go into debt or take from their savings to cover everyday expenses.

With economic uncertainty, fraud fighters need to prepare their companies for further friendly fraud. You need to:

ANALYZE
Which kind of first-party misuse is harming your company? Chargeback fraud? Refund fraud? Promo abuse?

ASSESS
What are your company's current policies around first-party misuse? How much harm is your company suffering as a result?

STRATEGIZE
How could it be improved? How can you identify friendly fraud more effectively? Dispute chargebacks more successfully? Deal with promo and returns abuse appropriately?

NEGOTIATE
Work with other parts of the organization to build a cross-company strategy that protects your long-term success.

COLLABORATE
Ensure all stakeholders are onboard with a plan that takes diverse needs into account.

IMPLEMENT
Make sure every department impacted takes the necessary steps. Communicate with customers as necessary.

PHISHING... FOLLOWED BY ATO

43%
of consumers were targeted last year by phishing scams or attempts to steal payment details.

220%
Increase of phishing incidents during the height of the global pandemic, compared to the yearly average.

148%
increase in ATO in 2021 on a year-over-year basis, fueled by the flood of phishing.

If consumers become more desperate, and less careful, during an economic downturn, fraudsters will have even more opportunity to launch successful phishing attacks.

Fraud prevention teams need to make sure they're prepared to repel an ATO uptick - even in cases where the "customer" has all the right static data that matches the account.

THE GIG ECONOMY OF FRAUD

Desperation also drives the gig economy of fraud - ordinary people tricked into playing an (often) unwitting role in a fraudulent scheme. When they need a job no matter what, they're less likely to examine whether an offered position might be too good to be true.

They might become:

ACCOUNT CREATION ACTORS
Setting up accounts on various sites and visiting them from time to time to age them and make them look legitimate - before passing control to the fraudster.

MONEY MULES
Enabling a fraudster to move money through their account, laundering it, or even setting up a new account for the purpose.

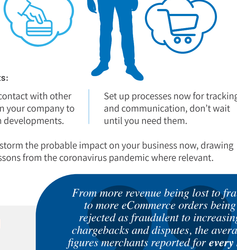
UNWITTING FRAUDSTERS
Making actual purchases online with stolen credit cards, given to them by the fraudster as being supposedly cards associated with the fake "business" that's employing them.

PARCEL MULES
Receiving stolen goods to their home address, and repackaging them and sending them on to the fraudster.

AND MORE ...

CHANGES IN USER BEHAVIOR

Consumers are extremely sensitive to economic shifts. A downturn will affect which products they buy, how much they buy, and where they buy them.



Every industry is different. To stay on top of shifts:

Track trends in your industry, outside of fraud.

Keep in close contact with other departments in your company to stay synced on developments.

Set up processes now for tracking and communication, don't wait until you need them.

Put plans in place - now - so you're prepared for different possibilities.

Brainstorm the probable impact on your business now, drawing on lessons from the coronavirus pandemic where relevant.

INVEST IN FRAUD PREVENTION

Many departments will be facing cuts. Fraud fighters need to convince the business that fraud prevention shouldn't be impacted. Simply put, you need to show that they can't afford to.

From more revenue being lost to fraud to more eCommerce orders being rejected as fraudulent to increasing chargebacks and disputes, the average figures merchants reported for ***every key indicator*** *tracked in the survey increased over the past year globally, on average*

Merchant Risk Council

- Make sure you communicate internally that fraud is impacting e-commerce more than ever
- Track all your metrics. Be able to show, at a moment's notice, how much loss you prevented this week, this month, this quarter
- Be proactive about helping to improve customer experience, including for new users -demonstrate that your department contributes to the bottom line

WE'RE ALL GOING TO KEEP HOPING FOR THE BEST, BUT WE ALSO NEED TO PREPARE FOR THE WORST. BECAUSE YOU KNOW THE FRAUDSTERS ALREADY ARE.

Sources:

- ACFE - Coronavirus Pandemic Is a Perfect Storm for Fraud
- WSJ - Business Owners Find New Ways to Crack Down on Shady Shoppers
- The Real Cost of Online Fraud, Ponemon Institute and Paypal
- Business Owners Find New Ways to Crack Down on Shady Shoppers - https://www.wsj.com/articles/SB10001424052748704533904574582103031039526
- NRF - 4 Things Retailers Need to Know About Inflation
- MRC Global Payments and Fraud Study 2021
- MRC Global Payments and Fraud Study 2022
- 2021 Fraud Report, Marqeta
- Phishing and Fraud Report, F5
- Imperva Bad Bot Report, 2022

www.identiq.com hello@identiq.com US +1 212 365 5638 UK +44 020 3997 0335