How fraud is shifting and how to respond

Risk and the COVID-19 pandemic

The COVID-19 crisis represents one of the biggest disruptions in the history of the electronic payments sector.

With GDPs falling, a global recession underway, and a change in consumer behaviors likely, many aspects of credit and debit card lending will be impacted. But, in the short term, it is the sudden shifts in the risk environment that are likely to have a profound effect on overall business performance.

Visa Consulting & Analytics (VCA) has investigated the changing face of electronic payments risk from several angles. In this paper, we focus on fraud management.

Almost every accomplished risk manager will have some experience of working through an economic downturn. Some may also have coped with a full-blown economic crisis, such as the global financial crisis of 2008 and 2009. While we have yet to determine the full extent of this unprecedented crisis, what is remarkable is the impact on everyday consumer behaviors.

In early May, for example, Oxford Economics reported that global household spending had fallen even further and faster than GDP[1]. Meanwhile, the payments industry news service PYMNTS.com reported that, in a period of just eight weeks, it had observed: "six times more consumers working from home, four times more consumers buying groceries online instead of going into the grocery store, four times more consumers ordering takeout from aggregators or their favorite restaurants, and three times more consumers shopping online for things other than groceries."[2]

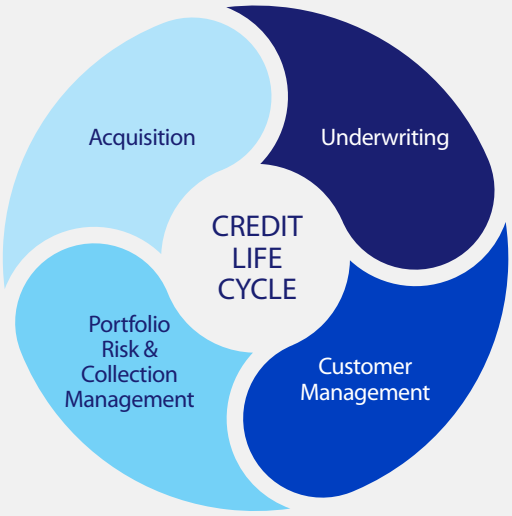
For fraudsters, the confusion, distraction and vulnerability stemming from the COVID-19 crisis spells opportunity. They can hide among the behavioral shifts, take advantage of the fact that banks and merchants alike are shifting gears, and prey on unsuspecting consumers.

For a risk manager it is a perfect storm. It is putting extreme pressure on all phases of the credit life cycle, all at the same time. To aggravate matters, there is real uncertainty as to how the crisis will evolve, how long it might last, or what the recovery could look like.

The COVID-19 crisis puts extreme pressure on all four phases of the risk cycle

With a shift in the economic fundamentals, there's a need to re-think the risk appetite, tighten the acquisition policy, and reduce the cost of acquisitions.

With increased risk across the portfolio, volume is pushed towards the collections function —which is the final back-stop in protecting performance and reputation.



As new risks materialize, there's a need to re-work underwriting models, think harder about risk-based pricing, and pay particular attention to origination fraud.

As customer behaviors evolve, customer management practices must follow suit —including credit line management, repayment plans, authorization management, and fraud detection.

1 "Coronavirus Watch As restrictions ease, a slow revival", Oxford Analytics, May 4, 2020: http://resources.oxfordeconomics.com/coronavirus-watch-as-restrictions-ease-a-slow-revival?oe_most_recent_content_download_id=0000029&interests_trending_topics=coronavirus

2 "Why Consumers Aren't In A Rush To Reopen The Economy", PYMNTS.com, 4 May 2020: https://www.pymnts.com/coronavirus/2020/no-rush-to-reenter-physical-world/

The payments industry is therefore experiencing a deep and sudden shift in the nature of electronic payments risk. In the short term, this shift is predicted to have a profound impact on the overall performance of any electronic payments business. In this paper, we focus on customer management, which encompasses fraud detection and fraud management.

There are three key points in regards to fraud detection and fraud management.

1 First, and most significantly, the current situation is fertile ground for fraudsters.

Types of activity reported include brute force attacks, ATM-cash-out attempts, phishing scams, and spurious cryptocurrency purchases, donations, and click-and-collect exercises. All the while, cyber security incidents continue to be a serious cause for concern. Issuers, merchants and acquirers must stay alert to the full gamut.

This adds to the fact that fraud rates do tend to be higher in the ecommerce channel, so any shift in the mix of card-present (CP) to card-not-present (CNP) payments will likely bring an increase to the overall fraud-to-sales ratio.

2 Second, many of the systems used by fraud managers are rendered less useful by the crisis.

For example, on the fraud detection front, many tools look for out-of-pattern spending. Yet, during the crisis, almost all spending is out-of-pattern. So, the proportion of false-positives inevitably spikes.

3 Third, issuers, merchants and acquirers should also brace themselves for a rise in first-party fraud.

A proportion of customers are facing real financial hardship, and some may be tempted to challenge legitimate transactions. Similarly, with locked-down consumers engaging in online shopping sprees, there could also be an increase in buyer's remorse, and a subsequent 'tide effect' of claims and disputes. An increase in application fraud should also be anticipated.

Meanwhile, with the rise of CNP transactions, an increase in 'friendly fraud' is perhaps inevitable. As cardholders review their statements, they may encounter transactions that look fraudulent – such as growth in categories not historically purchased online, merchant names that are not descriptive enough to connect the item purchased with the transaction amount, and multiple charges relating to a single purchase (for example, if retailers split charges based on the purchase amount and the shipping charges).

While it is too early to evaluate the full impact, the payment industry is bracing itself for a significant disruption. For example, several large payment processors are reportedly holding back deposits to hedge against an expected increase in chargebacks and, in the wake of the crisis, US cardholders are said to be disputing transactions at two to three times the previous level[3].

The challenge for the risk manager is to be extra-vigilant, and adapt to the new realities, but to maintain the quality of the customer experience. At a time when payment behaviors are changing, and new habits are likely to be formed, an over-zealous approach to fraud management could easily nudge a consumer towards using a different card.

3 "Hit by Coronavirus—and a 30% Holdback by the Payment Processor", Wall Street Journal, 15 June 2020: https://www.wsj.com/articles/hit-by-coronavirusand-a-30-holdback-by-the-payment-processor-11592040601

Universal Truths

While we have yet to determine how the crisis will evolve and what the long-term impacts may be, we can rely on some universal truths.

When it comes to payment, consumers have always cared – and will always care – about the optimum combination of trust, convenience, speed, simplicity and universal acceptance.

Meanwhile, the fraud management function always has – and always will – revolve around three inter-related parameters:

These three parameters will continue to determine the role and activity of the fraud management function. The shape of the triangle may be shifting, but the fundamentals remain the same. The task of the risk manager is to maintain the balance and equilibrium.

While the specifics of the response will be determined by the issuer's circumstances, the size and character of its portfolio, the fraud environment in which it operates, and the severity of the crisis in its home markets. VCA has compiled nine imperatives that, we believe, are relevant to any issuer operating anywhere.

Nine imperatives for fraud teams in the COVID-19 pandemic

#1

Be prepared for account testing exercises – like enumeration or brute-force attacks

Right now, this is perhaps the biggest risk of them all.

Fraudsters are using the global surge in ecommerce volumes as cover for their account testing exercises. Through enumeration or brute force attacks, they are systematically sending authorization requests to an issuer's BIN to deduce legitimate payment credentials.

So, look out for any unusually high growth in transaction counts. Pay attention to declines for invalid account numbers, and look out for flurries of regular authorization requests (e.g. one every few seconds from the same source).

If you suspect an attack is underway, act fast to get the situation investigated. Also, look out for authorization requests using sequential account numbers and provide extra protection to any similar numbers.

#2

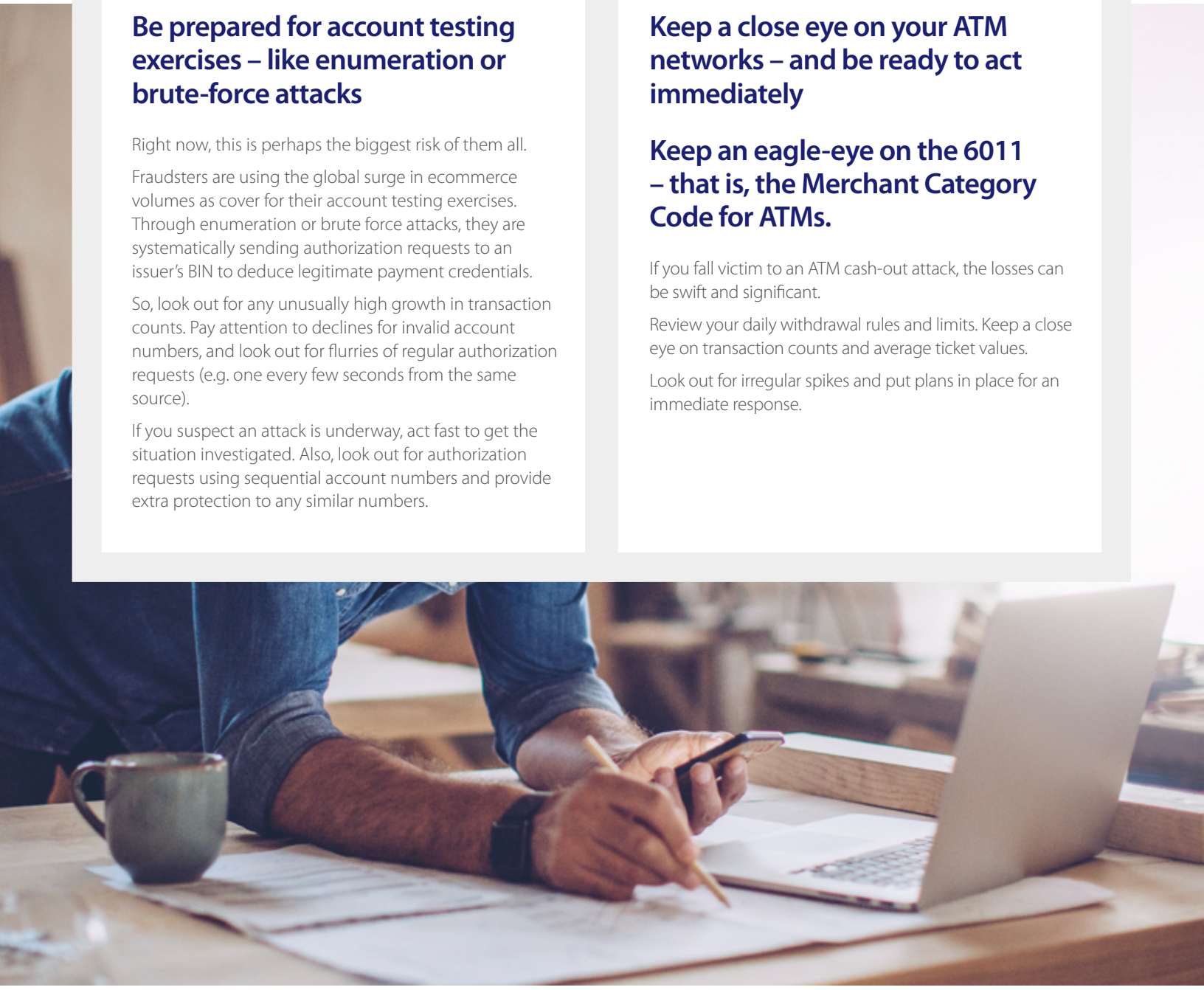
Keep a close eye on your ATM networks – and be ready to act immediately

Keep an eagle-eye on the 6011 – that is, the Merchant Category Code for ATMs.

If you fall victim to an ATM cash-out attack, the losses can be swift and significant.

Review your daily withdrawal rules and limits. Keep a close eye on transaction counts and average ticket values.

Look out for irregular spikes and put plans in place for an immediate response.



#3

Partner with the wider ecosystem – and help your peers to help you

A united, sector-wide approach is one of the best defenses we have. Be sure to actively engage with any industry forums and law enforcement, and reach out to your peers to evaluate trends and possible solutions.

Also, be super-vigilant with your fraud reporting. The sooner you file your reports, the sooner the Visa systems can learn from them. Through tools like Visa Advanced Authorization (VAA) and Visa Risk Manager (VRM), emerging risks can be suppressed before they become full-blown trends.

#4

Be aware that any gaps in your armor can be quickly found and exposed

Fraudsters will be probing for vulnerabilities in the way you run your operations and protect your portfolios.

If, for example, you do not have overnight or weekend coverage in your fraud operations teams, now might be the time to extend their hours. Similarly, if your people are working from home, but do not have access to the tools and technology that is available to them onsite, you may want to provide some back-up.

Also, pay close attention to the risks faced by your vendors. If, for example you outsource some of your fraud operations to a third party, how are they coping with the crisis?

At times like this, your ability to manage fraud should be optimized – not compromised.

#5

Inform, educate and encourage your cardholders

Use all channels to communicate proactively with your cardholders – and take the opportunity to both educate and reassure them.

Let them know that, because you are being extra-vigilant, they may receive more fraud related communications and/or verification requests than normal.

Also, warn them about any fraud types that are prevalent or emerging in your market. Also, remind them of any alert or SMS services you provide.

#6

Lean on your analytical resources

The key to identifying new or unknown fraud patterns most likely lies in your existing transaction data. So continually challenge your analytics teams to find new insights.

Most fundamentally, you probably want to speed up your existing reporting cycles, moving from quarterly or monthly, to weekly or daily.

In addition, pre-COVID-19, your CNP fraud rates were most likely skewed due to the high volume of travel transactions. To get like-for-like comparisons, you should strip out the travel transactions, which will most likely be miniscule in the post-lockdown environment.

#7

Deal sensibly, systematically and swiftly with the increase in fraud alerts

It is inevitable that you will receive a high volume of risk alerts. You should accept that (due to the mass shift to ecommerce and a surge in out-of-pattern spending) your risk scores will lose some of their potency.

So, reassess your performance rules to reflect the forced change in everyday payment behaviors and prioritize your investigations activity.

Also, move quickly to update your risk models. For example, supervised fraud models will need to be tweaked quickly and more frequently due to changing behaviors. With almost all spending being out-of-pattern due to COVID-19 and the increase of false-positives spikes, you should report new fraud as soon as possible, include new findings, and calibrate accordingly.

And, if you are still using rules-based techniques, this should be a wake-up call to modernize using the latest data assets, tools and technologies.

#8

Revisit your crisis management and cyber-event plans in light of COVID-19

Your crisis management plans, contingency plans, and cyber security assessments were most likely formulated under very different circumstances. It makes sense to take a look at them through a COVID-19 lens and work out what and how you would change.

For example, how quickly and efficiently could you deal with a sizeable compromise or a significant cyber-event? How exposed could you be? Would your teams and system capabilities be up to a rapid response?

#9

Don't forget the human touch

If the worst should happen, and an account becomes compromised, be open and proactive in your customer communications. Usually, they will expect:

- To be to informed if fraud takes place
- To be believed
- For everything to be resolved within days
- To be kept informed every step of the way
- To be guided through the recovery process
- To receive advice on how to prevent fraud from taking place in the future

It is also an opportunity for you to turn a potentially difficult situation into a reason for customers to stay loyal.

While the COVID-19 pandemic has affected businesses everywhere, opportunities can arise from challenging situations. Visa Consulting & Analytics can advise on how your business can best respond to the COVID-19 pandemic.

VISA

About Visa Consulting & Analytics

We are a global team of hundreds of payments consultants, data scientists and economists across six continents.

- Our consultants are experts in strategy, product, portfolio management, risk, digital and more with decades of experience in the payments industry.
- Our data scientists are experts in statistics, advanced analytics and machine learning with exclusive access to insights from VisaNet, one of the largest payment networks in the world.
- Our economists understand economic conditions impacting consumer spending and provide unique and timely insights into global spending trends.

The combination of our deep payments consulting expertise, our economic intelligence and our breadth of data allows us to identify actionable insights and recommendations that drive better business decisions.

For help addressing any of the ideas or imperatives above, please reach out to your Visa Account Executive to schedule time with our Visa Consulting & Analytics team or send an email to **VCA@Visa.com**. You can also visit us at **Visa.com/VCA**.

