White Paper

Fraud Triage in the COVID-19 Crisis

What Banks Can Do to Respond

Kevin Knott, Brian O'Malley, Scott Barton, Dave Wasik, Matthew Barton and Ankit Mathur

August 2020

As the depth of the COVID-19 crisis became apparent in mid-March, lenders appropriately focused on credit challenges, from how to handle new origination credit contraction and managing the effects of COVID. Meanwhile fraudsters were closely monitoring lender responses searching for new vulnerabilities and identifying the perfect opportunity to strike.

Early on, as banks were forced to shift to work-from-home models, many had call center capacity decrease by 25% or more. The impacts have been mostly mitigated as employees have become more efficient at home, but with banks having to manage increase in load across multiple functions (e.g., customer care), fraud staffing remains constrained. For lenders looking to scale up capacity, training has been a challenge, as use of tools, internal resources, and coordination across units are more difficult to teach and reinforce remotely.

At the same time, existing transaction fraud models are suddenly less effective, as they have been built on a pattern of behavior that the shutdown significantly altered, and which continue to change as COVID-19 closings and re-closings evolve. As lenders looked to proactively adjust their cut-off scores to get ahead of new fraud attacks, the breakdown of models, driven by many more online purchases and fewer card-present transactions, has led to more customer transaction declines and increased volumes of outbound contacts. A similar story played out with application fraud. As lenders scaled back new origination volume and there was an overall drop in customer demand, 1st and 3rd party application fraud models started to break down. For those lenders that relied on face-to-face branch interactions to resolve identity fraud concerns, they quickly found themselves with a backlog of cases as branch hours were cut back or closed altogether.

As expected, fraudsters have attempted to exploit the situation with many lenders experiencing an increase in fraud attacks across multiple fronts. As noted in American Banker, "credit and debit card fraud rose 35% in April from a year earlier"[1]

This paper shares insights into two broad questions:

1. What are new or adjusted strategies being perpetrated by fraudsters during the COVID pandemic?
2. How should lenders respond in combating these types of attacks?

[1] https://www.americanbanker.com/news/identity-fraud-is-soaring-heres-how-one-lender-is-attacking-it

Emerging trends in fraud due to COVID-19

Fraud experts relate fraud loss mitigation to squeezing a balloon. As the external environment and a lender's fraud capabilities shift over time, they're effectively squeezing on one end of the balloon only to see a massive bulge in another area as fraudsters quickly adapt and find a new weakness. The current COVID-19 crisis has quickly cut off two traditional fraud targets - new applications and in-store card present transactions driven by muted lending activity and shift of consumer spends to online respectively - thus forcing criminals to quickly adapt and find new weaknesses to target. We are currently seeing this play out as criminals have locked in a on a few areas:

1. BIN Attacks / Online Fraud: Fraudsters don't just execute broad-based mass attacks where they think there might be vulnerability, they instead use sophisticated low-cost test-and-learn strategies to constantly ping each bank's fraud defenses, looking for any vulnerability. Then when they find one, they capitalize on it with a highly pointed attack. Technology advances have enabled fraudsters to execute exponentially more attacks without increasing costs, causing banks to respond with increased defenses in the constant arms race escalation. With lower store traffic and many locations closed, on-line attacks have once again become a focal point for criminals as they can easily execute these attacks from the comfort of their home.

One such example is Bank Identification Number (BIN) attacks where fraudsters generate new card numbers using a specific BIN number and try out all the new numbers with low value transaction amounts to identify which cards are active. As the crisis hit, one bank was seeing hundreds of thousands of BIN attack attempts per day until they implemented stricter CVV mis-match decline rules which we believe is a key step in ensuring exposure to such attacks are mitigated. Not surprisingly, volumes dropped by over 95%, as fraudsters retreated to more of an ambient level of attacks.

BIN attacks are one example, but criminals are also looking to exploit online fraud more broadly. As consumer spend shifts aggressively to online channels, criminals are able to hide within the massive uptick in volume in order to avoid detection. As an example, address mis-

match between the shipping address and address on file for the consumer is historically a strong risk splitter; however many consumers are choosing to shelter in place with other family members or away from their primary residence. As a result, lenders are seeing increases in false positive rates from address mis-match rules which also increases the ability for criminals to slip by undetected.

2. Bogus merchants: Fraudsters moved quickly to set up new fake merchant IDs. They knew that institutions, including Payment Card networks and Associations, were likely to be overwhelmed and might take longer to identify and shut them down. Many of these were initially set up around legitimate sounding "hot' products like personal protective equipment and have more recently shifted to bogus charities looking to cash in on consumers looking to donate to health and social causes. We expect the definition of "hot" product will keep changing over the course of the crisis as in-demand items continue to shift e.g., the next "hot" category could be treatments or vaccines once they're available. So it is important for issuers and acquirers to be cognizant of this trend and react accordingly to it.

3. Disputes and Friendly Fraud: Just as in previous downturns, card issuers are seeing an increase in true name customers disputing legitimate purchases, especially on internet purchases delivered to the home, which have increased with the stay-at-home guidelines. There also was a spike in travel-related disputes, as customers looked to card issuers for help or as a last resort in trying to reclaim money for travel that was cancelled. There was one prominent travel site which simply posted an interstitial page notifying customers that all travel was canceled and telling them to contact their bank to discuss options available to them as a cardholder.

4. Application Fraud: While not nearly as pervasive as transaction fraud attacks, fraudsters have continued to look for opportunities to monetize hacked and synthetic identities through online applications. With most banks pre-emptively tightening fraud flow-down rules for applications, we haven't seen a spike here yet, although we know that some lenders who maintained higher origination volumes have seen an uptick in their attack rates. Despite the lack of broad industry upticks, we have some wariness about heightened attacks as banks relax previously tightened underwriting standards once they're ready to re-enter the market. Early movers who quickly expand channels that were closed, will need to monitor for new attacks.

5. Account Takeover Fraud: As many lenders have scaled back originations making it more challenging to commit application fraud, criminals have shifted to leveraging stolen personal information to take over existing accounts. As part of the shift to account takeover, there has been a spike in phishing attempts by fraudsters, capitalizing on increased digital communication as everybody is working from home. The increased email volume makes it harder for corporate email filters to decipher good from bad and increases the likelihood that a consumer may click on a link in an email that they may not have if they could quickly validate the authenticity with the IT person in the office. Criminals have also pounced on the opportunity presented by consumer interest in receiving stimulus checks from the government via direct deposit vs. waiting on a paper check. Criminals have ramped up phishing emails offering quick and easy access to stimulus funds if they provided their checking account information of where they want to receive the funds. As a result, several financial institutions have reported an uptick in account takeover attempts across servicing channels, as criminals' cash in on successful phishing attempts.

6. Internal Fraud: One issuer already has seen a marked increase in employee committed fraud as call centers moved to work-from-home status without the proper system functionality and monitoring in place to deter and detect these internal breaches. The temptation for employees to commit internal fraud is only likely to increase as we get further into the recession and government stimulus runs out, putting increased stress on families impacted by loss of income.

What Banks Can Do to Respond

Enhance models to adapt to the current environment

Transaction fraud models "learn" from previous data and don't react well when baseline "good" behavior changes rapidly. Online purchases have surged since stay-at-home policies, and card-present transactions, especially far from customers' homes, have fallen dramatically. So an online transaction for a large order may look out of pattern pre-COVID-19, but is more likely to be a good transaction today, just as a large purchase far away from a card-holders' home, especially if it's international, is much riskier today than it looks to the model (especially if the cardholder used to make international trips). As states begin to re-open at different rates (and as some potentially roll back re-opening), the ability of these variables to predict fraud will change quickly. Whereas in certain geographies, percentages of Card Not Present transactions may quickly shift back to their pre-COVID-19 levels, in other locations it will take much longer. This type of quick changes in data and its predictive power will require lenders to be nimble in their approach to using models.

While eventually lenders will want to recalibrate or rebuild models based on more up to date data, that will be difficult as conditions continue to change. Subsequently, leading lenders are looking to update their policies and/or implement overlays to existing rules such as:

- Geo-distancing triggers
- Analysis of online false negatives and false positives by merchant type including more stringent rules & monitoring for new untested merchants that could be bogus
- State-by-state or region checks to incorporate different levels of stay-at-home behaviors

By identifying new emerging patterns before models can pick them up, banks can shut down attacks earlier. Also, as discussed in a later section, tuning models to individuals rather than consortiums (e.g. is this customer buying from specific online merchants now) allows banks to de-average their fraud triggers, saving money and creating better customer experiences (e.g., preventing a customer from getting "good" transactions flagged by the bank's rules).

As part of the rule recalibration process, banks need to revisit their current decline rules for CVV mismatches with an eye toward tightening. Best practices include analyzing merchant types where there has been spikes in BIN attacks and tightening rules there. Some banks strategically still approve transactions with previous CVV for customers who may still be using an old card. As other banks tighten in this way, those that don't will find themselves even more subject to attacks.

Banks can also leverage targeted 2-way SMS strategy to retain spend for good customers who get flagged by fraud defenses, generally referred to as false positives. One major issuer has had great success with this strategy, both in gaining more spend they would have lost, as well as in seeing much higher Net Promoter Scores for this population. An additional best practice is to record which customers are making these "good" transactions without CVV post COVID-19 and feed that data back into their models as to when to allow spend for those customers at those merchants. One institution was sending some customers as many as 10 alerts in a month because they weren't tracking rules at the customer level – not surprisingly, customers who are contacted that frequently react poorly in terms of future card use.

Finally, in addition to stopping transaction fraud, authorization rules are a critical component of a well-designed account takeover prevention strategy. Issuers should review recent account changes as an input to transaction fraud detection and deterrence. A best practice is to treat differently two customers who look alike and make the exact same transactions, but one has had a recent account change (e.g. phone number update, or worse, multiple failed attempts at changing account data). Incorporating account level data into the account take-over scoring is a critical element of account take-over prevention.

Harness the power of advanced modeling methodologies

An important decision for banks is the degree to which they let their models "learn" vs building new models and decision rules. This depends on many factors, including the learning speed of the models, how quickly the bank updates scores, and how flexible their models are in allowing modifications. Industry standard is refreshing models every 6-12 months which will not be adequate given the rapid changes going on now and for the next several months. Banks with the most advanced Machine Learning models have a distinct advantage in surgical accuracy and speed of model updates, and we are seeing them

distance themselves in terms of losses from other banks. One leading practice is de-averaging more surgically across accounts and merchant types through cutting edge modeling, lowering losses and seeing fewer fraudster attacks as they learn this bank is a tougher target.

More surgically de-average false positives

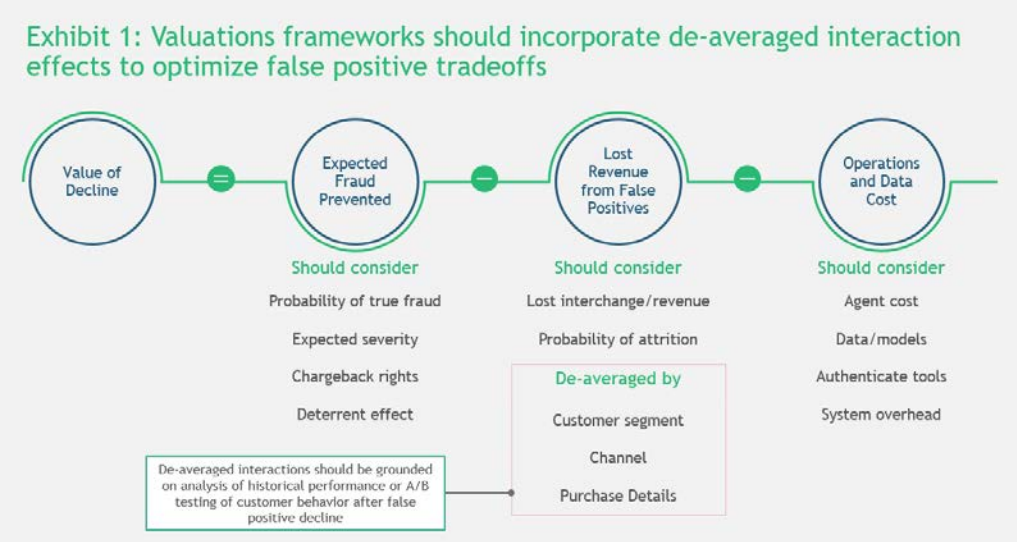
A key part of any bank's transaction fraud prevention strategy is systematically optimizing the rates of "false positive" declines, i.e. "good" transactions that the bank's controls thought were "bad". All major issuers use a false positive target (e.g. 10:1 ratio), and all de-average by segment to ensure that the rules are not being applied bluntly. But best in class issuers have more granular rules that look at purchases at the customer level to optimize fraud decisions in order to minimize lost revenue and bad customer experience. Institutions with 10:1 target have some sub-segments with <3:1 ratio and others with >100:1.

The most effective approach is to leverage more advanced modeling techniques (see above) and a granular segmentation to more effectively realize their targeted ratio. As noted in Exhibit 1, we recommend issuers should, at a segment level, develop a valuation framework to optimize false positive trade-offs considering expected fraud prevented, lost revenues from false positives and operations cost.

For example, declining a borderline transaction for a low credit risk customer who regularly revolves high balances may be very unprofitable. Meanwhile declining the same transaction for someone in that same cohort who never revolves and is showing higher credit risk behavior, may be profitable.

One important yet challenging component of a valuation framework is to incorporate the impacts of fraud deterrence. Many lenders will look at the fraud losses directly prevented by the strategy but don't consider the fraud that was never attempted because criminals realized there was a more stringent policy in place thus pushing them to target other lenders or fraud types. Quantifying the impact of deterrence is nearly impossible but high-level assumptions can be created based on factors such as how visible the strategy is to a criminal, if a new rule is directly addressing a vulnerability vs. tweaking an existing rule, or how the new rule positions the lender relative to peers. One institution is distancing itself from peers by de-averaging more surgically across accounts and merchant types through

cutting edge modeling, lowering losses and seeing fewer fraud-attacks as criminals learn this bank is a tougher target.



Embrace the robust and rapidly developing ecosystem of data vendors

There has been much innovation in the data space, as vendors are tapping the growing array of information on customers (e.g., cell phone proximity to attempted transaction, etc.). There is a myriad of vendors, and testing their products is time consuming but can create risks if a bank is unable to leverage a tool or data source that has become industry standard. Banks should focus on several areas to tap into this ecosystem.

- Maximize advanced device intelligence: on transaction fraud, the key is maximizing access to advanced device intelligence. This may sound somewhat obvious but is really challenging to do in practice given the speed requirements in the authorization flow. One cutting edge lender has been able to increase fraud captures rates while also dramatically reducing false positive declines by assessing whether the customer is using a device that has been associated with the account in the past.

- Behavioral analytics: In the application fraud space, behavioral analytics is key. Examples include measuring the time to complete each field in the application (really fast and really slow being risky, along with the same time for many fields), looking for copy/pasting of key personal information such as SSN, or tracking cursor movement around the application page — fraudsters have upped their game in doing robo

applications and banks need to keep elevating their defenses in response. We have even seen more advanced lenders measure the tilt of the mobile device or amount of pressure being applied to the device as an input to risk. The possibilities of incorporating behavioral data are almost limitless so it is important for a lender to have a solid strategy to identify value of incremental behavioral data while also keeping the customer experience and their privacy in mind.

- Embrace internal data: Although getting access to high leverage 3rd party data is critical, it's equally as important that lenders fully embrace the vast amount of internal data available in their decisioning engine. One large issuer attributed over 50% of the application fraud that they stopped to internal bad lists despite leveraging multiple 3rd party fraud scores. Lenders offering multiple products should create enterprise repositories of consumer information and bad lists to improve performance and prevent criminals from jumping between products.

- Finally, lenders should also stay up to date on the progress the Social Security Administration is making around the implementation of the electronic Consent Based Social Security Verification (eCBSV) service and integrate that into their verification process once the data is available.

Migrate to seamless, digital customer authentication solutions (and finally retire ineffective solutions such as Knowledge Based Authentication)

Identity fraud, including stolen and synthetic identities, has been on the rise for the last few years and has increased as COVID-19 pushes more banking interactions digital. Combine this with the fact that consumers in general and especially high spend populations, expect a fast and frictionless experience has put increased pressure on lenders to create digital, seamless identity verification processes across the customer lifecycle. Many Fintechs have already moved in this direction but it will be especially challenging for larger lenders that rely on face-to-face branch interactions to resolve identity concerns.

Lenders should look to integrate digital identity document verification solutions as a foundational component at application stage and for high risk account changes. There are many solutions in the market that can effectively verify the legitimacy of the ID in real time

in order to let good customers quickly continue in the process while weeding out the bads. While these types of solutions are prevalent enough in the market that most consumers are willing to accept the increased burden for the sake of security, it is critical that lenders are able to complete the identity verification process on the first try otherwise they risk the consumer abandoning the process. This is especially true for lower risk and higher spend consumers who can easily find access to credit at another lender.

In addition to document verification, one-time PIN via SMS is another option that is both reasonably secure and relatively frictionless for good consumers. But it is not foolproof so it should only be used to resolve lower risk concerns and where possible, lenders should leverage push notifications via the mobile app as a replacement for sending a SMS message.

Conclusion

There are clear indications that criminals are probing for new vulnerabilities created by COVID-19. While the most sophisticated issuers have been able to weather the increase in attacks with relatively little impact, issuers that are less sophisticated in their fraud defenses are already seeing significant impact. Credit risk is appropriately the first concern of CRO's in a post COVID-19 word, but improving fraud defenses can be done quickly and can net >$50M per year in savings for many issuers. It is critical that lenders don't lose sight of the fraud risks as they remain focused on credit losses and navigating the economic downturn. Fraud teams should consider the following points when adapting their program to the current economic environment:

- **Rule Management**: Build a suite of fraud rules based on geography, purchase amount, distance from home, etc. to supplement your core risk model. Continually refresh rules as states relax stay-at-home orders and acquisitions teams relax their underwriting criteria as they enter growth mode. Uncertainty around the accuracy of credit bureau data will not only impact effectiveness of underwriting strategy but potentially increase fraud risk as risk models no longer identify fraud attempts that were previously credit declined.
- **Differentiated Treatment**: Lenders need to sharpen their fraud defenses but do so surgically so that they still maintain strong customer experiences. Blunt rule tightening could alienate customers and damage long-term value so there is a need to be targeted in adjusting any rules or policies. Strategies should incorporate customer segment, transaction type, deterrence, etc. to limit friction on more sensitive interactions.
- **Advanced Analytics**: Develop custom machine learning models to identify anomalies/trends relative to current observations. Incorporate leading edge data sources to improve performance and get ahead of criminals instead of reacting to attacks.
- **Reduce customer friction** by focusing on seamless, digital first verification solutions that are effective at mitigating risk while minimizing customer friction.

- **Monitoring** is more important than ever in order to quickly identify and react to emerging threats. Lenders should leverage flexible solutions that can quickly adapt to the evolving fraud landscape.

Kevin Knott
Brian O'Malley
Scott Barton
Dave Wasik
Matthew Barton
Ankit Mathur

Kevin Knott is a Sr. Business Director at 2nd Order Solutions where he leads the fraud practice; he has over 14 years of experience in credit and fraud risk management and has led the implementation of best in class fraud models for Capital One's US Card portfolio. Brian O'Malley is a Managing Director & Partner in BCG's Minneapolis office, he is core member of BCG's Risk practice and global leader of Collections topic. Scott Barton is the Founder and Managing Partner at 2nd Order Solutions where he has led many dozen Collections projects for major banks and FinTechs, he previously was one of a handful of Senior Credit Officers at Capital One and led Collections, Recoveries, and Fraud. David Wasik is a Partner at 2nd Order Solutions, he has over 25 years of credit and lending experience and led Collections and Recoveries for Capital One's US credit card division during the Great Recession. Matthew Barton is a Principal and core member of BCG's Financial Institutions and Risk practice areas and is based out BCG's Philadelphia office. Ankit Mathur is a Knowledge Expert in BCG's Financial Institutions Practice with a focus on Payments and Transaction Banking segment and is based out of BCG's New York office.

You may contact the authors by e-mail at:
Kevin.knott@2os.com
OMalley.Brian@bcg.com
Scott.Barton@2os.com
Dave.Wasik@2os.com
Barton.Matthew@bcg.com
Mathur.Ankit@bcg.com

About BCG

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we help clients with total transformation—inspiring complex change, enabling organizations to grow, building competitive advantage, and driving bottom-line impact.

To succeed, organizations must blend digital and human capabilities. Our diverse, global teams bring deep industry and functional expertise and a range of perspectives to spark change. BCG delivers solutions through leading-edge management consulting along with technology and design, corporate and digital ventures—and business purpose. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, generating results that allow our clients to thrive.

About 2OS

2nd Order Solutions (2OS) is a boutique credit risk advisory firm that specializes in solving the world's most challenging credit problems. 2OS was founded 12 years ago and consults to a wide range of banks, card issuers, fintechs, and specialty finance companies in the US and abroad.

2OS has deep experience with lending businesses across Card, Auto, Small Business, and Personal Loans, at all points in the credit lifecycle. 2OS partners have vast expertise in all aspects of Collections, both as operating executives and as consultants.