KOREFUSION

The Evolving U.S. Debit Landscape:

A Focus On Authorization Fraud & Network Perceptions

The Evolving U.S. Debit Landscape: A Focus On Authorization Fraud & Network Perceptions

The US debit landscape is undergoing a period of change as regulators, consumers and payment providers drive evolution across the ecosystem. Numerous critical factors have catalyzed the current debit network landscape in the U.S. Among them, the Durbin Amendment, which passed in 2011 and was updated in July 2023 to include several provisions, now requires at least one unaffiliated network on each debit and prepaid card.

The rapid evolution of online transactions, further accelerated by the pandemic, has made online transactions all but ubiquitous in today's society, even when we may not explicitly realize we are engaging in an online transaction – for example, when we hail a ridesharing service. These online transactions, otherwise referred to as Card Not Present (CNP) transactions within the industry, have required the payments ecosystem to adapt to how it identifies and reacts to CNP fraud. By many metrics, the industry still has much catching up to do relative to card-present fraud, with 4x more CNP fraud taking place in 2021 globally than card-present fraud[1].

Facilitating the ongoing growth of CNP transactions requires, in part, evolving the industry's approach to fraud identification and screening to optimize the balancing act of deterring true fraud while limiting the friction between the consumer and merchant for a seamless purchase experience online. To that end, in this paper, KoreFusion set out to offer insights specifically into how debit card issuers manage fraud on inbound CNP transactions. Our secondary goal was to capture how the various U.S. debit networks are perceived by the issuer ecosystem, if one puts pricing aside, to understand where performance or capabilities expectations are met, exceeded, or fall short.

This paper provides an overview of the current U.S. debit network landscape, followed by a summary of our key findings regarding how debit card issuers manage fraud detection and scoring in CNP transactions, the role of payment processors to that end, and how networks are positioned when it comes to their CNP capabilities.

KoreFusion spoke with a range of U.S. debit card issuing entities, including banks and fintechs, as well as the payment processors and core banking that support debit card issuing operations and inbound fraud scoring. We spoke with roughly 20 institutions that range in size from national players to local community banks and credit unions – to ensure diversity of inputs and perspectives.

Our approach is rooted in a framework by which to categories the various types of U.S. debit networks:

- Global Front-of-Card Networks: The "front-of-card" global networks; Visa, Mastercard,
- Affiliated Back-of-Card Networks: Interlink (owned by Visa), Maestro (owned by Mastercard),
- Unaffiliated Back-of-Card Networks: NYCE, STAR, Pulse, Accel, Shazam, etc.

The global networks of Visa and Mastercard operate their respective "front-of-card" networks and acquired Interlink and Maestro, their respective affiliated "back-of-card" networks, in 1991 and 1994, respectively. The unaffiliated networks originated as ATM networks that later developed PIN-based point-of-sale capabilities to enable their cards to be used for in-store purchases. Many unaffiliated networks have recently developed the capabilities to process transactions without a PIN (PINless) allowing them to do so in both an online and offline environment.

It's also important to note that payment processors own and operate many of the unaffiliated, back-of-card networks. For example:

- Accel – Owned and operated by Fiserv
- STAR – Owned and operated by Fiserv
- NYCE – Owned and operated by FIS
- Pulse – Owned and operated by Discover Financial Services.

This consolidation between payment processors, who themselves are often core banking providers (in the case of Fiserv and FIS), and debit networks, impacts how issuers engage in the unaffiliated network selection process. In many cases, the unaffiliated network selection is the by-product of a broader technology and operational relationship between the issuer and the payment processor where a wide range of card and banking operations are being outsourced to these infrastructure providers.

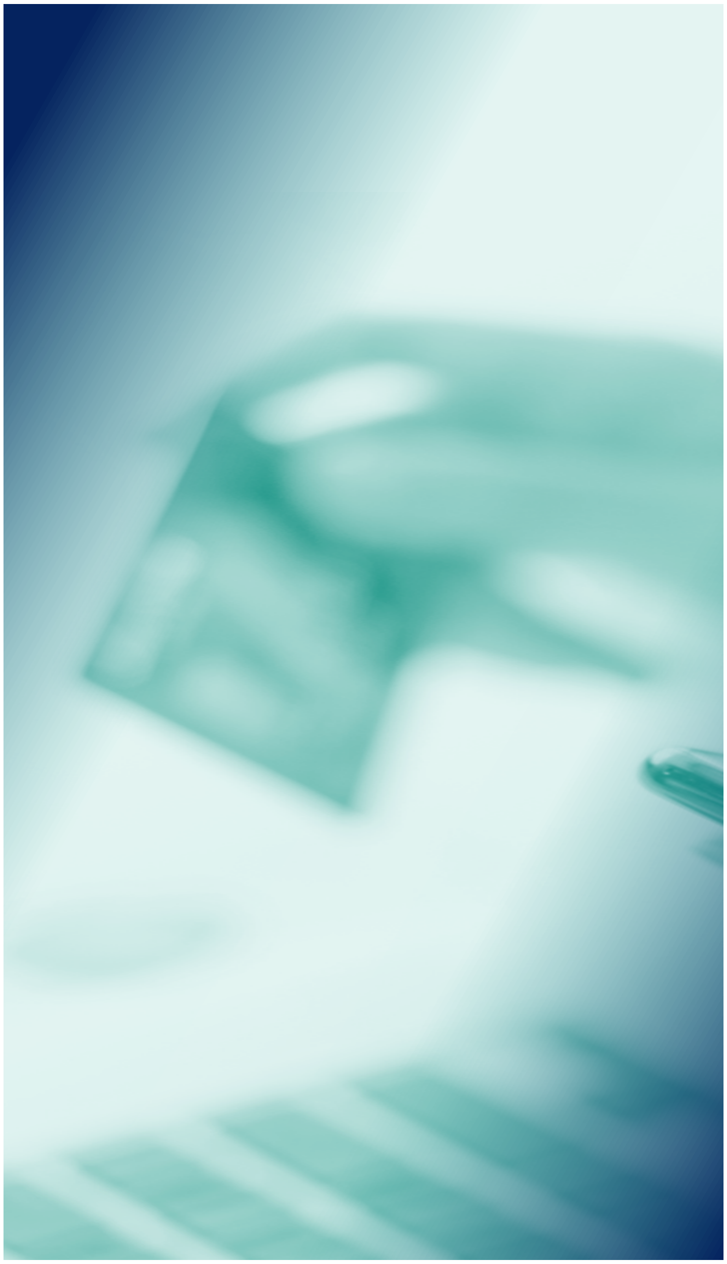
[1] Visa Navigate, "The Card Not Present Balancing Act

U.S. Debit Network Landscape Snapshot

When possible, larger merchants often prioritize which debit network its transactions are routed to and, historically, made this choice based on authorization rates, network rules, fraud rates, and cost, amongst other criteria. These differentiators – particularly fraud protection and authorization rates – have skyrocketed in importance as CNP volumes increase and merchants bear the liability for CNP fraud per most network rules.

The unaffiliated back-of-card debit networks (e.g., NYCE, STAR, Pulse, Accel, etc.) – which were mostly limited to ATMs and physical point-of-sale transactions and are relatively new to online commerce – have CNP growth in their sights. To access this market, they are introducing and expanding the footprint of their PINless Debit solutions to enable the use of their networks for CNP transactions.

While merchants bear the liability for CNP fraud, as per the network rules for virtually all the debit networks, the issuing banks still bear significant costs related to fraud, including fraud mitigation services, dispute management & resolution services, customer service channels, and brand exposure. Therefore, it is important for issuers to understand how the debit networks they choose to work with may impact, positively or negatively, their direct and indirect fraud costs.



The Focus Of This Whitepaper

Most critically, we aimed to uncover how issuers approach the fraud scoring aspect of this process, and how the process for balancing in-house systems versus outsourced fraud solutions and scoring algorithms is evolving. Subsequently, we also explored the industry-wide implications of these shifting approaches for banks, payment processors, and debit card networks.

As the unaffiliated networks attempt to play a larger role in CNP transactions, we wanted to understand if debit card issuers – be it banks or fintechs – had strong perceptions about the relative strengths and weaknesses of the unaffiliated networks versus the global & affiliated networks. We also sought to understand what impact fraud management has as debit networks compete for CNP market share now that two competing debit networks must be present on all U.S. debit cards due to recent updates to the Durbin Amendment.

The Growing Sophistication Of Online Fraud Has Forced Most Banks & Processors To Utilize 3rd Party Fraud Protection Solutions

Online fraud is an increasingly complex and sophisticated issue that is playing out on a national and international scale. Most banks, even many large ones, don't feel they have a substantial enough line of sight through their own debit card portfolios to keep in-house fraud systems up-to-date and effective enough in the face of ever-evolving threats.

In response, fraud monitoring and detection systems are becoming equally sophisticated and specialized to combat fraudsters, and this level of specialization makes it increasingly more challenging to manage fraud in-house. Issuers are increasingly turning fraud management over to the 'experts'.

Barring the largest national banks and some select banks and fintechs with unique cardholder portfolios, issuing banks have largely chosen to outsource the inbound debit authorization fraud checks to their payment processing partners. These processors use a variety of tools – including network-generated fraud scores, third-party fraud solutions, and in some cases, proprietary fraud tools.

"As a smaller bank we find ourselves at conflicting ends of the spectrum. On one hand, we are too small to absorb fraud losses the way bigger banks can – it has a direct and material impact on our financial performance. But we also recognize our regional debit footprint isn't sufficient to build proprietary anti-fraud capabilities, so we need to trust external vendors to manage this critical task for us."

— EVP of Card Operations (Regional Bank)

"Fraud is playing out on an international scale with highly sophisticated fraudsters requiring highly sophisticated anti-fraud technologies to combat them. Even as a nationwide bank, we know it isn't possible to build this expertise in-house. We partner with best-in-class providers and work very closely with them to develop and refine a layered anti-fraud system that is customized to our portfolio."

— Head of Debit Operations (National Bank)

Our outsourced anti-fraud system is heavily reliant on the fraud scores provided by the inbound debit network and it is complemented with open-source data sets, integrations with best-in-class partners, and our bank and account specific watchlists and blacklists."

— Former Risk Officer (Super-Regional Bank)

What's more, these processing partners - particularly FIS and Fiserv – play an outsized role in fraud detection and scoring across banks of all sizes. While we expected to see a larger proportion of smaller banks rely on payment processors for various debit card services, we found that many mid-sized and large banks also utilize them to manage the fraud aspect of their debit authorization process.

Payment Processors (and very large issuers) have invested heavily in orchestrating their fraud detection and scoring systems. Their strategy for supporting the evaluation of debit card authorization requests includes linking proprietary datasets with open-sourced fraud tools, leveraging the debit network-generated fraud scores, and integrating best-in-class third-party fraud solutions into their tech stacks. Additionally, the payment processors' scale provides them with a substantially broad line of sight across a wide range of payment transactions and fraud types that allow them and their 3rd party providers to train their fraud solutions against the largest possible datasets.

Payment Processors Dominate In Providing Banks Fraud Detection & Scoring Orchestration

In addition to internal fraud detection and scoring systems, many processors have white label integrations with various third-party fraud solutions, which bank clients can easily plug into to augment and expand the processor's internal tools. In all cases, the processors' fraud systems were reliant on the fraud score generated by the inbound debit network as part of the data payload transmitted with the debit transaction authorization request. (All the debit networks offer some form of fraud scoring, but as seen in the next section, the dependability and false positive rates of these fraud scores could differ between debit networks.)

This positions payment processors as convenient and valuable outsourcing partners for banks to manage debit card authorization fraud. Banks can utilize their client contracts and define SLAs to manage their payment processors' performance. Additionally, most payment processors have portals that allow their bank clients to manage their fraud thresholds and fraud strategies (up to a point), enabling them to offer customizable outsourcing offerings to their issuing clients.

> There is a broad range interaction levels that our issuing bank clients choose to have with our fraud platform. Some banks like to actively manage fraud thresholds, A/B test, and segment their card bins to manage fraud risk. An equal number of banks have never utilized their fraud portals and leave the management of their fraud systems entirely to us."
>
> **— SVP, Card Services (Leading Payment Processor)**

This trend towards outsourcing of fraud management means that the majority of debit card operations systems within banks is now limited to account-specific checks, which occur as a result of fraud scores and / or recommendations from a payment processor partner. These account-specific checks typically include verifying the debit card number, confirming adequate funds are available in the linked cardholder's account to complete the transactions, and completing final bank-specific watchlist / blacklist checks.

In sum, banks have limited-to-no upside in managing fraud in-house. Effective fraud management requires continuous investment of resources to maintain the status quo of limiting fraud losses: a best-case scenario. On the other hand, one misstep puts banks in the hot seat with liability and a poor customer experience. Leveraging external vendors relieves banks of the internal resource burden and responsibility for fraud events.

Unaffiliated Debit Networks Fall Short On Fraud Scoring

The global debit networks were largely seen as superior to the unaffiliated debit networks regarding generated fraud recommendations, which served as a key input for all anti-fraud systems. This is due, in part, to the inherently global reach and scale of the global debit networks. The inclusiveness of this dataset provides sufficient volumes to develop and continuously evolve sophisticated fraud detection / scoring algorithms and precision tuning of fraud tools.

Several banks in the study referenced the lower false positive rate seen through the global networks compared to the unaffiliated networks, which made them more confident in the fraud recommendations generated by the global networks. Among the global networks, some banks were even more specific in calling out the lower false positives seen in Visa's fraud recommendations versus Mastercard's.

Many banks that had customized thresholds for authorization fraud recommendations between the global, affiliated, and unaffiliated networks have had to develop internal workarounds to compensate for the less accurate fraud score generated by the unaffiliated networks.

> "We closely monitor the false positive rates and overall accuracy of the debit scores we receive from the four different debit networks we support. We do this, in large part, so we can adjust various thresholds in our fraud platform to reflect the variability we see between network-generated fraud scores. In our experience, Visa and Mastercard have lower false positive rates and noticeably more accurate overall fraud scores versus the unaffiliated networks. Slicing it even finer, we find Visa's scores are incrementally more reliable than Mastercard's."
>
> **— Head of Fraud Analytics (Super-Regional Bank)**

Capabilities, Network Economics Hinder PINless Debit Rollout

Economics notwithstanding, the global debit networks were seen as superior or equal to the unaffiliated debit networks across a number of key characteristics

The uptime of the unaffiliated networks was widely criticized as being below expectations, regardless of contractions obligations / SLAs.

Issuers we spoke with indicated uptime was a primary concern, vocalizing praise for the uptime of the global and affiliated networks (vs. the unaffiliated networks). The relatively substandard uptime of unaffiliated networks means issuers effectively need to rely on Stand-In Processing (STIP) rules when those go down, which issuers report as poor and resulting in unnecessary declines.

Alternatively, reliance on a network with strong uptime provides merchants with a better customer experience by limiting unnecessary declines resulting from STIP. The issuer also gets more accurate fraud protection in real time.

> *"While it should be a table stakes topic, network uptime is one of the most important issues for us when comparing the debit networks. The uptime of the unaffiliated networks is meaningfully worse than the global and affiliated networks, and the stand-in-processing rules for the unaffiliated networks are rudimentary. This causes problems for our cardholders and merchants with unnecessary declines."*
>
> ***— Head of Card Operations (State-Wide Bank)***

Issuers reported poor or non-existent automated chargeback and / or dispute resolution tools from unaffiliated networks. In contrast, issuers praised global networks for the value, sophistication, and efficiency derived from their automated chargeback and dispute resolution tools.

Numerous banks specifically called out Visa as having a particularly robust toolkit in this area – a key reason they were pleased the vast majority of their inbound debit transaction volumes come through Visa and not an unaffiliated network.

Similarly, merchants – which are inevitably involved in the dispute and chargeback resolution processes – benefit from the robust dispute resolution tools of global debit networks. A well-automated, digital toolkit for dealing with these issues at scale streamlines dispute resolution for merchants who can dedicate fewer manual resources to dealing with this costly issue. This is particularly acute for high-velocity online merchants who cannot possibly manage the chargeback process manually.

> "[A global gaming console] can hit a high-water mark of approximately 10,000 chargebacks in a given week within the U.S. alone. There is no way they can handle this volume of disputes without a highly sophisticated and automated dispute management platform."
>
> **— Former Fraud Executive (Top 5 U.S. Issuing Bank)**

From the unaffiliated networks' perspective, their network economics and competing internal investment priorities have caused the PINless debit rollout process to go slower than anticipated, making it difficult for them to play a meaningful role in CNP transactions.

Unaffiliated networks are focusing on larger merchants in their efforts to promote PINless debit adoption; however, these merchants already closely manage interchange and payment acceptance costs, rendering any potential cost-related benefits from PINless a minimal point.

On the issuer front, the promotion of PINless debit capabilities is progressing more slowly than anticipated. This is due, in part, to competing priorities, but also because the business case is difficult for the issuers to make; the lower interchange economics of PINless debit makes it a lower revenue product than the global debit network offerings.

Conclusion

While many issuers and merchants may not spend much time thinking about the debit networks they choose to work with, fraud-related liability borne by these banks and merchants will continue to grow proportionally with the growth of CNP. This phenomenon suggests that the choice of debit network, with their varying degrees of fraud management capabilities, merits further scrutiny and attention.

The issuing banks we spoke with indicated that the fraud scoring systems and dispute/chargeback management tools offered by the global networks are superior to those provided by the unaffiliated debit networks and can create meaningful economic and operational value for issuers, fintechs and merchants.

The global networks have carved out a differentiated position for themselves with regard to the quality of their fraud scoring and recommendation engines (as well as their dispute/chargeback automation platforms). To maintain this differentiated position, global networks could continue to invest in these capabilities and remain at the forefront of anti-fraud technology (e.g., ML & AI). In tandem with this effort, global networks might prioritize communicating their investments and commitment in this space to issuers, fintechs, merchants and payment processors.

Our findings also highlight the increasingly critical role payment processors are playing as the outsourced fraud platform of choice for issuing bank clients, which rely on them to make debit authorization decisions. Similarly for merchants, who utilize these same processors to handle their payment acceptance capabilities.

CNP PINless debit adoption and rollout remains limited. Without a broader network efforts flywheel in place, unaffiliated network volumes for CNP transactions will likely remain low (sub-20% of most banks' CNP debit volumes), and their lack of visibility into a large enough CNP dataset will continue to hamper the unaffiliated networks' ability to improve and fine-tune their fraud scoring systems.

About KoreFusion

KoreFusion uniquely combines strategy consulting and M&A advisory services exclusively for the international fintech, payments, and financial services industries. KoreFusion works with leading corporates, banks, payment networks, fintechs, processors, payments enablers & infrastructure providers, and ERPs / digital business platforms worldwide to address their emerging challenges around payments and financial technology from both a strategy and M&A perspective.

For more information on KoreFusion's payments and Fintech research, please contact:

information@korefusion.com

San Francisco · New York · Mexico City
São Paulo · Dubai · Singapore · Mumbai

www.korefusion.com