CHEAT SHEET

- *Impending operations.* There has been a notable increase in initiatives set forth by the US Federal Trade Commission and the US Consumer Financial Protection to cut off "bad merchants" from the payment system. This trend is sometimes referred to as "Operation Choke Point."
- *Preventative measures.* There are many steps that processors and ISOs can take to mitigate the risk of litigation, including: (1) carefully monitoring chargeback ratios, (2) being wary of multilayered or complicated merchant structures, (3) documenting departures from credit policies, and (4) reviewing online complaints and chargeback narratives.
- *The merchant class action.* In recent years, the plaintiffs' class action bar has become fixated on the complex pricing models that processors and ISOs use to deliver services to merchant customers. When faced with a merchant class action suit, in-house counsel should review the processing agreement, reevaluate sales training, and consider arbitration.
- *Chip tech.* The transition to EMV or "chip" cards in the United States was a hasty process that left many merchants without the certified equipment. As a result, the merchant that accepts the card bears the risk of the chargeback.

THE ONSLAUGHT OF LITIGATION IN THE PAYMENTS ACQUIRING INDUSTRY

(AND HOW TO MITIGATE RISK)

By Theresa A. Vitello, Edward A. Marshall, and Theresa Y. Kananen The acquiring side of the payments industry — comprised of the banks, payment processors, and independent sales organizations (ISOs) that recruit and service merchants wishing to accept credit and debit cards — remains relatively obscure in the public consciousness. These players facilitate trillions of dollars in transactions and provide the rails on which the modern consumer economy operates, but they do so quietly. When all goes as planned, they merely reside in the background of every payment card transaction, whether it takes place at a traditional brick-and-mortar establishment or an online retailer.


RISK
1
2
3
4
5
6
7
8
9
*
0
#
V

For years, litigation activity involving these entities has reflected this relative anonymity. Aside from the occasional lawsuit involving a disgruntled merchant or an unhappy business partner (or, at worst, legal wrangling following a data breach), processors and ISOs rarely found themselves staring down a significant litigation threat. Over the past four or five years however, things have changed. Government actors seeking to hinder businesses engaged in "undesirable" consumer transactions have taken aim at the processors and ISOs that allow those businesses to accept payment cards. The class-action bar has begun to see the industry as a potential source of lucrative challenges (after all, when any individual defendant helps facilitate the flow of billions of dollars, attacking even a per-transaction rounding error may be an attractive fight). Additionally, the card brands (e.g., Visa and MasterCard) have rolled out "chip" cards in the United States — which is the most complex and fractured payment system in the world — on an incredibly compressed timetable, altering the allocation of risk for counterfeit transactions as a result of this more robust fraud-prevention technology. The friction created by these changes, perhaps unsurprisingly, has landed where Americans gravitate in times of uncomfortable change: the courts.

In short, the litigation risks facing the payments industry are graver now than they have ever been — but those risks can be effectively mitigated. Preventative maintenance within an organization, coupled with experienced counsel on the front lines, can materially reduce a processor or ISO's exposure to the growing threat. This article explores how.

Regulatory enforcement actions (a.k.a. Operation Choke Point)

Perhaps the most existential threat a processor or ISO can face is a regulatory enforcement action by the US Federal Trade Commission (FTC) or the US Consumer Financial Protection Bureau (CFPB). Referred to (albeit at times too loosely) as "Operation Choke Point," recent initiatives by these government bodies spawned from the realization that cutting off "bad" merchants' access to the payment ecosystem is an effective way to shut down companies engaged in consumer deception (think bogus peddlers of miracle nutraceutical products, online coaching programs, or debt-relief scams that trap vulnerable consumers into recurring monthly charges for worthless or nonexistent deliverables). Thus, the government has looked to augment enforcement actions against the unsavory merchants through the exertion of pressure on processors and ISOs who work with the (perceived) bad actors.

The objectives animating these regulatory actions may be understandable — even laudable. Not all consumers are savvy enough to understand that they have the legal right to "chargeback" bogus transactions, leaving a large number of individuals victimized and uncompensated by unscrupulous businesses. And, to be fair, there have always been some bad apples in the payments space that have worked a little too hard to keep bad merchants in business with the hope of maintaining an income stream in the form of processing fees and/or residuals.

At the same time, however, the increasing ferocity with which the FTC and the CFPB have come after the payments space, and the apparent attempt to deputize industry players as surrogate agency watchdogs, has drawn a fair amount of criticism. A historical overview helps to understand the ungirding of these criticisms.

Historical development of Operation Choke Point

Historically, processors and ISOs were merely asked to assist the government in its pursuit of unsavory merchants by responding to subpoenas and civil investigative demands. That made sense. Chargeback histories, to which processors have access, can illuminate just how disgruntled consumers of a merchant's goods or services have become. Underwriting files can shed light on merchant ownership, and how scammers have structured their organizations to avoid effective oversight by the card brands (which have their own interests in aggressively ferreting out and shutting down consumer fraud).

This state of affairs lasted until recently, when the government decided to get more aggressive. It began to seek *ex parte* asset freezes over merchant assets, and slip in language purporting to require the turnover of processor

Theresa A. Vitello is vice president and assistant general counsel at EVO Payments International.
theresa.vitello@evopayments.com

Edward A. Marshall is a partner at Arnall Golden Gregory. He serves as chair of the firm's business litigation team and is co-chair of the firm's payment systems practice.
edward.marshall@agg.com

Theresa Y. Kananen is a partner at Arnall Golden Gregory. She is part of the firm's litigation and employment practices and serves as a co-chair of the firm's payment systems practice.
theresa.kananen@agg.com

"reserves" associated with the merchant (i.e., processor holdbacks, typically a percentage of merchants' transaction volume, designed to protect against processor liability for chargebacks that the merchant ultimately proves unable to satisfy).

Such asset freeze orders remain a sore point of contention between the government and the processing community. Without affording processors due process and depriving them of reserve funds, which would otherwise be available to satisfy chargebacks and other losses related to the merchant account, seems wrong. And whether due to disputes as to the ownership of reserve funds or the presence of perfected first-priority security interests, the legal foundation for treating those funds as subject to seizure is substantively questionable. Despite this tension, the impact of these regulatory actions was considered manageable until recently. The amount in controversy rarely reached seven figures, and most regulators and government-appointed receivers were willing to compromise on the demands in light of their shaky legal footing.

Ratcheting the regulatory pressure up further, however, the government more recently began pursuing processors and ISOs (along with individual principals) as defendants in cases alleging unfair and deceptive practices against merchant co-defendants —seeking to hold them liable not just for the revenues associated with "bad apple" merchants, but for the entirety of the consumer harm perpetrated by their merchant customers (in the form of the totality of the merchant's transactions, minus only returns and chargebacks). That, of course, increased the risk to an almost unbearably high level. Processors and ISOs that received just a tiny fraction of the merchants' transaction volume in revenue (much less profit) faced liability exposure orders of a magnitude higher than what principles of disgorgement would ordinarily permit.

Faced with such high stakes litigation, processors, ISOs, and individual principals were forced (and continue to be forced) to settle rather than risk non-dischargeable, catastrophic liability exposure. As a consequence, courts have had little opportunity to rule on the permissibility of such seemingly disproportionate relief. The case law remains less than clear, with some courts appearing to endorse such disproportionate remedies (under the innovative theory of "joint and several equitable disgorgement") and others expressing skepticism at the legal justification for such draconian sanctions.

Notably, a recent back-and-forth between the Middle District of Florida and the 11th Circuit in *FTC v. WV Universal Mgmt., LLC, et al.*, Civil Action No. 6:12-cv-1618 (M.D. Fla. filed 2012), may soon shed some light on whether processors and ISOs who are not part of a "common enterprise" with their merchant customers can actually be forced to "disgorge" revenues orders of a magnitude higher than what they received. *See FTC v. HES Merchant Servs. Co., No.* , No. 15-11500, 2016 WL 3254652, at *1 (11th Cir. June 14, 2016); *FTC v. WV Universal Mgmt., LLC, et al.*, Civil Action No. 6:12-cv-1618 (M.D. Fla. Oct. 26, 2016). Given the number of courts in which the government has pursued such relief, however, and the number of fact patterns underlying those challenges, it may be years before any clear standard emerges from the courts.

Proactively protecting your organization

As the acquiring community awaits judicial clarity on just how far Operation Choke Point will be permitted to go, there are proactive steps that processors and ISOs can take today to mitigate their exposure. Protection starts not just in the legal department, but in underwriting and risk.

Such asset freeze orders remain a sore point of contention between the government and the processing community. Without affording processors due process and depriving them of reserve funds, which would otherwise be available to satisfy chargebacks and other losses related to the merchant account, seems wrong.

Carefully studying the allegations of countless complaints filed by the FTC and the CFPB against processors, ISOs, and their principals reveals a pattern of perceived "red flags" — alleged acts or omissions in the underwriting and risk monitoring processes that, with the benefit of hindsight, the government contends show reckless disregard (or worse) of consumer interests. Adjusting those processes in collaboration with legal and risk departments, while unlikely to completely exclude all bad merchants from the ecosystem, can both help avoid consumer harm and make a processor or ISO a less likely target of regulatory ire.

Cataloguing all of the best practices that can be deduced from the government's filings would be a Herculean undertaking (and make for a really boring article), especially because they can vary significantly across different merchant verticals.[1] But a few deserve special attention:

- **Carefully monitor chargeback ratios:** To the extent there is anything constant about the government's attacks on processors and ISOs, it is failing to address high chargeback ratios (i.e., the ratio between reversed transactions versus total transactions). While there has been no magic percentage

identified at which chargebacks transform from merely a credit risk to be contained into cause for regulatory concern, and no magic duration for those ratios to persist before the government deems it "too long," ratios approaching or exceeding the double digits that persist for months — despite attempts at mitigation — open up an acquirer to significant regulatory scrutiny. Thus, when a merchant remains stuck in a card brand monitoring program, or when stubbornly high chargeback ratios cannot be resolved through merchant counseling, it may be time to pull the plug on the processing relationship.

- **Be wary of multilayered or complicated merchant structures:** Fairly or not, the government often cites the presence of multiple merchant accounts (MIDs) or fractured merchant structures as a "red flag" that should be more thoroughly vetted as part of the underwriting process. The same is true with regard to complex corporate architectures, especially those having an inexplicable multinational reach. Although there are numerous reasons why such arrangements can be perfectly valid, untoward merchants have used these structures to obscure principal ownership and to provide for "fallback" accounts — sales channels that can continue operating if others are shut down (e.g., for excessive chargebacks). Thus, as part of the boarding process, merchants should be pressed to be transparent about their structures and to provide legitimate explanations for the need to spread business across multiple MIDs. In any event, processors and ISOs should take care to ensure that their partners and sponsoring banks are apprised of the reasons for such structures. The government is quick to cite lack of transparency with business partners as evidence that a defendant knew, or recklessly disregarded the possibility, that merchants were up to something shady.
- **Departures from credit policies should be considered and documented:** Credit policies — whether internally generated or handed down from processing partners — should not be lightly disregarded. There will certainly be times when it makes sense to consider boarding merchants whose verticals are deemed "high-risk," or times where substandard credit scores, involuntarily terminated processing relationships, or even hits in the MATCH database should not disqualify a merchant from consideration. When those instances do arise, processors and ISOs would be well advised to document the reasoning that led to those approvals — ideally augmented by monitoring plans to ensure that a potential credit risk does not in fact perpetrate consumer fraud. In that regard, principal guarantees — even those backed up by reported wealth — are no substitute for diligent underwriting and risk monitoring.
- **Review online complaints, reviews, and chargeback narratives:** The government is fond of citing negative online reviews or disturbing chargeback narratives as overlooked (or consciously ignored) indicia of consumer fraud. While it may well be infeasible to monitor all, or even most, merchants' online ratings or chargeback descriptions, making such reviews part of the response to excessive chargeback ratios can make good sense. Clever merchants know how to dupe their processing partners as well as the consuming public, and often can offer plausible sounding explanations for a few months of higher-than-anticipated chargebacks (such as, e.g., consumer confusion regarding the business name appearing on their credit card statements). When those chargeback ratios are accompanied by negative online reviews (such as on the Better Business Bureau or *ripoffreport.com*) or chargeback narratives that suggest something shady is taking place, however, they can be useful data points to consider in deciding whether to continue attempts at merchant remediation or to instead terminate the processing relationship.

Making sure risk and underwriting departments are aware of these potential "red flags" can dramatically reduce the threat of becoming ensnared in the web of Operation Choke Point.

Making sure risk and underwriting departments are aware of these potential "red flags" can dramatically reduce the threat of becoming ensnared in the web of Operation Choke Point. Better yet, implementing systems where complicated underwriting and risk-monitoring decisions are made as part of a dialogue between business and legal (whether in-house or outside counsel) can ensure that such decisions are both well-informed and, where appropriate, protected by attorney-client privilege.

The rising merchant class action threat

About the same time that regulatory enforcement actions became a fixture on the payments litigation landscape, another equally disturbing trend began to take shape: the merchant class action.

Specifically, over the past three to four years, the plaintiffs' class action bar has become fixated on the sometimes complex-pricing models pursuant to which processors and ISOs deliver services to merchant customers. At least in certain corners of the industry, the plaintiffs' bar contends that acquirers are inflating "costs" (such as interchange) in purported cost-plus pricing models, roping merchants into processing agreements with promised savings that never materialize. Other times, they have seized on specific pricing increases, challenging fee hikes that were ostensibly designed to recapture pass-through costs but, allegedly, built in undisclosed profit margins for processors or ISOs.

To date, most of these class actions have settled (with no admission of liability), so the accuracy of the merchants' challenges is open to question. That said, if the allegations are true, such litigation has the potential to benefit the industry by ensuring greater transparency and honesty in comparative pricing presentations — making sure that processors and ISOs do not lose footing to competitors based on mythical promises of cost saving.

Like Operation Choke Point, these class actions have more recently veered into less justifiable challenges. In at least a few instances, merchants have initiated putative class actions that attack the industry with a hatchet instead of a scalpel, taking issue with everything from how terms and conditions are communicated to merchants, to how necessary price increases are implemented, to how merchants are compelled to promptly alert their processors to perceived fee discrepancies (e.g., within months after receiving a statement, as opposed to years after the fees were charged). These cases have also tossed around accusations of unconscionability — like confetti at a parade — taking issue with industry-standard limitations periods for initiating suit and the allowance of attorneys' fees for prevailing parties.

Again, how these lawsuits will ultimately shake out for the industry is open to prognostication. Most of the cases are still in their infancy, and more mature cases have often settled, either on individual bases or (in more extreme cases) in class-wide fashion. But, as with regulatory enforcement actions, there are steps that processors and ISOs can take now to reduce the litigation threat. These include:

- **Reviewing the processing agreement:** Many of the plaintiffs' challenges to processing agreements

seem altogether unlikely to succeed, but there is always value in dusting off processing agreement templates and evaluating the enforceability of various clauses in light of the emerging litigation landscape. As class action litigation and regulatory enforcement actions highlight points of contention, minor tweaks to templates that bolster enforceability can save significant legal spend down the road in defending provisions of questionable validity.

- **Reevaluating sales training:** No processor or ISO can effectively script out every interaction between its sales force and the merchant customer base. However, taking time to document "dos" (e.g., ensuring the merchant acknowledges receipt of terms and conditions) and "don'ts" (e.g., improperly characterizing certain fees as costs) can help establish that undesirable sales techniques are unreflective of company policy. At a minimum, when a sales agent goes rogue, highlighting the departure of his or her conduct from company policy can help establish that the relevant merchant's experience was atypical (and not one pervasive or consistent enough on which a class can be certified).
- **Considering arbitration:** The enforceability of generic class-action waivers is still an open question; the enforceability of arbitration clauses that mandate one-on-one dispute resolution, thankfully, is not (except in California, where certainty tends to remain elusive). While abandoning the courts in favor of private dispute resolution is a weighty and complex decision, processors should at least consider whether the rise of merchant class actions has altered the arbitration calculus enough to make arbitration, coupled with a class-action bar, a desirable alternative.

The next wave? EMV disputes

Any user of payment cards has noticed the increasing prevalence of chip cards and terminals that accept (or proclaim they will soon be ready to accept) EMV or "chip" cards. These chip-enabled cards are far more difficult to replicate than their magnetic stripe predecessors, making them an effective weapon against the billion-dollar problem of counterfeit fraud (at least in card-present environments). These cards are expensive to manufacture and even more expensive to accept, however. Thus, to spur adoption of EMV (or "chip") card technology in the United States, the card brands have to date opted against any sort of rule-based mandate, and instead have attempted to nudge the industry toward chip adoption through "liability shifts."

Historically, when criminal organizations stole payment card information and manufactured counterfeit cards, liability for fraudulent transactions was shouldered, first and foremost, by the banks that had issued the legitimate but easily replicated card (the card brands came up with elegant solutions to recapture some of those losses from the sources of any data breach that gave rise to the counterfeiting, but that story is for another article). After October 2015, at least for most card-present credit card transactions, that changed. Now, if an issuing bank has given a consumer a chip-enabled card, and some ne'er-do-well makes a magnetic-stripe replica of that card, the merchant that accepts the card (because such merchant doesn't yet have EMV certified equipment) bears the risk of a chargeback.

The migration to EMV, however, has been anything but smooth. Card issuers have run into bottlenecks getting chip-enabled cards manufactured. Many merchants waited until the eve of the liability shift to seriously consider upgrading point-of-sale equipment, and processors (along with their service providers and the card brands) have struggled mightily to certify all the terminals, gateways, and servers that must be reprogrammed, recalibrated, and thoroughly tested to make EMV-card acceptance a reality. Finite resources, coupled with the need to individually certify thousands of different components in the most complex and fractured payment system in the world, left many merchants without EMV-certified equipment for months — even years — after the liability shift went into effect.

ACC EXTRAS ON… Litigation

ACC Docket
Learning to Avoid Costly Wage and Hour Class Action Litigation (April 2017). *www.accdocket.com/articles/wage-and-hour-class-action-litigation.cfm*

Research Roundup: IP Litigation Forecast from Deanna Kwong of HPE (Jan./Feb. 2017). *www.accdocket.com/articles/research-roundup-ip-litigation.cfm*

Litigation Management: The Critical Steps to Achieve Success and Reduce Costs (Oct. 2016). www.accdocket.com/articles/resource.cfm?show=1438698

InfoPAK
Information Governance Primer for In-house Counsel (Oct. 2016). *www.accdocket.com/docket/articles/resource.cfm?show=1439795*

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT *WWW.ACC.COM*, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

Now, merchant frustration at that glacial pace and the accompanying exposure to chargeback liability is starting to bubble up into litigation — principally against the card brands themselves. In at least a few instances, however, merchants have gone after their processors, too, either as sources of information for the larger battle against Visa and MasterCard or, at times, as targets themselves for not expediting terminal certification to the merchant's liking.

As with Operation Choke Point and merchant class actions, the ultimate viability of these challenges will only be resolved with time and litigation, but there are ways to mitigate the exposure. Clear communication and transparency are key. Processors should remind their merchants that they did not set the liability shift dates and that nothing in the card brand rules or regulations actually requires EMV acceptance. Moreover, while projecting timetables for certification is an inherently inexact science, processors can explain how they are approaching the certification backlog — whether for point-of-sale terminals, ATMs, or pay-at-the-pump petrol terminals. Such communication may be of little solace to the merchant who is having to grapple with chargeback liability until the certification process concludes, but this approach can at least reassure merchants that their processors and ISOs are attempting to be part of the solution, and are not the source of the problem. Customer service and communication may the best tools acquirers have in their arsenal to grapple with the EMV quagmire.

Conclusion

The rise of litigation challenges facing the payments acquiring industry shows no sign of abating. Whether they take the form of regulatory enforcement actions, merchant class actions, or EMV disputes, the threats are real and the exposure can be significant. Proactive steps, developed jointly by legal, risk, underwriting, and marketing departments, can help to mitigate those threats and reduce the potential for significant liability exposure or outside-counsel legal spend. **ACC**

NOTE

1 For a more detailed discussion of best practices by merchant sector, consider reviewing the *Electronic Transaction Association's Guidelines on Merchant and ISO Underwriting and Risk Monitoring.*