4 TRANSACTIONAL POLITICS

Getting Paid and Not Getting Paid

In 2014, Eden Alexander had a severe reaction to a common medication. She was covered in blisters, and, as she put it, her "skin was peeling off like paint."[1] Dismissed by urgent-care workers and referred to a dermatologist and a psychiatrist, she soon developed a secondary MRSA infection. By the time a hospital admitted her, Alexander was in myxedema coma, a rare condition with a very high mortality rate.

During Alexander's recovery, she and her friends set up a crowdfunding campaign using GiveForward, a platform specifically designed to raise money for medical costs. But soon, Alexander was notified that her campaign had run afoul of terms of service and would be canceled, all donations refunded. What had gone wrong?

In the initial email, GiveForward notified Alexander that WePay, GiveForward's underlying payment service provider, had "flagged her account" as in violation of WePay's terms of service, which stated that it could not be used "in connection" with pornographic services. Eden Alexander is an adult performer. On her Twitter account, she described herself as a "multiple award nom'd Adult, Fetish, Bondage +Alt Model, FemDom, CamGirl. Teazeworld Girl! (Ultimate)Grand Supreme. Feminist Porn & BDSM director."[2] The GiveForward campaign, however, made no mention of her job and focused entirely on her medical expenses.

Alexander posted a screenshot of the email on her Twitter account.[3] Immediately, there was a flurry of tweets, blog posts, and news coverage criticizing WePay. Two days later, in response to the growing uproar, WePay published a post on its company blog, stating that its system had detected that Alexander had retweeted other supporters who'd offered adult material in exchange for donations to her crowdfunding campaign.[4] This was, according to the WePay blog, "in direct violation of our terms of service as our back-end processor does not permit it."[5] Alexander had indeed retweeted two supportive pornography companies: a studio that had offered a free video clip to anyone who donated $50 to Alexander, and a website that had offered a set of pictures to anyone who donated $20 or $50 and a year's membership to anyone who donated $100.[6]

In the blog post, WePay wrote, "Upon further review, WePay suspects Eden may not have been aware of the terms of service and we are offering her the ability to open a new campaign for further fundraising."[7] WePay did not enable her to restart the same campaign or collect any of the funds that had already been donated, nor did it explain the limits or scope of its social media monitoring. CrowdTilt, another crowdfunding site serviced by a different payments provider, Balanced Payments, offered to host Alexander's campaign, and she quickly raised over $10,000.[8]

WePay had originally made its name as the preferred payments processor of the Occupy movement, vowing not to surveil or freeze accounts associated with the protest movement the way that PayPal and the card networks had done to WikiLeaks.[9] Previously, staffers from WePay had criticized PayPal's notoriously opaque and inconsistently enforced terms of service by pranking the 2010 PayPal Developers Conference. They dropped off a six-hundred-pound ice sculpture filled with five-dollar bills that directed people to the WePay site UnfreezeYourMoney.com.[10] According to WePay, this stunt increased its user base by 225 percent.[11] At the time, WePay founder Rich Aberman described his company as the "anti-PayPal," in large part because of its better customer service around confusing account freezes.[12] In another ironic twist, WePay's origin story involves its founders

splitting the costs of a friend's bachelor party, an event that, as many of Alexander's supporters pointed out, would have probably included activities outside the bounds of its present terms of service.[13]

Many supporters of Alexander saw WePay's actions as overt discrimination against sex workers. The blogger and feminist porn star Kitty Stryker argued, "Because Eden is a cam girl, I guess she doesn't deserve fundraising." Stryker also noted that the WePay terms of service prohibited "adult or adult related content, including performers or 'cam girls.'" This wording, to Stryker, implied that Alexander had violated WePay's terms of service, "not by raising money FOR porn, but *by being a cam girl at all*."[14]

The Twitter hashtag that supporters of Alexander used was #whorephobia, a play on "homophobia," implying that WePay was afraid of the mere association with someone in Alexander's profession. There is plenty of evidence that such whorephobia exists and indeed is alive and well. As of 2018, the sex-worker activist Liara Roux has documented dozens of examples of financial service companies discriminating against sex workers.[15]

Others, such as civil libertarians concerned with privacy and freedom of information flows, were more concerned about the implications of WePay's surveillance-based business model. One poster on Reddit wrote, "My worst fear wasn't realized (that there is a sex worker blacklist being distributed by banks and money exchangers), but my second to worst fear was: they actively monitored her social media for an excuse to ban her (and used a retweet as the excuse)."[16] That there could be some sort of a "blacklist" for exclusion from payments was disturbing, but so was the prospect of private social media surveillance that would effectively accomplish the same thing.

In WePay's blog post responding to the uproar, the company argued that it did not take a moral stance against pornography or sex workers and that it had successfully managed crowdfunding campaigns for other pornographic performers in the past.[17] WePay cofounder and CEO Bill Clerico explained on Twitter that WePay had to follow the "rules set by banks, Visa & MasterCard." He also emphasized that WePay was "required to monitor

customer websites and social media [because] we have to, not [because] we want to."[18]

All of these reactions need unpacking. Alexander's supporters and others who were outraged at WePay's poor stewardship of payments were right that, in effect, it was a case of "a white tech bro deciding it's his place to take away money from a porn performer who needs medical care."[19] But Clerico was also right that Alexander was in violation of WePay's terms of service, which were embedded in multiple interlocking systems. But neither provides a satisfying explanation of how or why this happened.

Like many critical infrastructures, the systems that enable us to get paid are mostly invisible: we only notice them when they stop working.[20] When the systems of getting paid go wrong, it usually comes in the form of an account freeze. Those who face account freezes usually don't have a good sense of how or why it happened. Even when explanations are given, they may not be clarifying. As one observer put it, "The same as always: The 'system' has 'detected' an 'unusual' amount or frequency of money transferred. So they closed it for 'security reasons' and it will take days, if not weeks to reopen it again."[21] The technologies through which people get paid feel like black boxes to most users. The case of WePay not working for Eden Alexander when she needed it most provides an opportunity to move past the hot takes and figure out what went wrong and why.

Eden Alexander is not alone. Every day, countless people and organizations, for a variety of reasons, suddenly and unexpectedly find themselves cut off from the infrastructures of getting paid. And, as in Alexander's case, the consequences can be dire.

The power—and politics—of not getting paid is well illustrated by the controversy around "Operation Choke Point," a 2013 partnership between the US Department of Justice and the multiagency Financial Fraud Enforcement Task Force. Established by President Barack Obama after the 2008 financial crisis, the task force targeted fraud and consumer predation in financial institutions by constraining merchants' ability to get paid. As one Justice Department official described it, "We are changing the

structures within the financial system that allow all kinds of fraudulent merchants to operate," with the intent of "choking them off from the very air they need to survive."[22] The first major action under Operation Choke Point came against a North Carolina bank that had processed payments for Ponzi schemes.

Immediately, Operation Choke Point was met with opposition from Republican lawmakers and certain sectors of the financial services industry. California Republican representative and head of the House Oversight Committee Darrell Issa stated that the "true goal" of Operation Choke Point was not to combat fraud but to "'choke out' companies the [Obama] Administration considers a 'high-risk' or otherwise objectionable."[23] He held up as evidence task force documents that described gun and ammunition sales as "high risk." On the other hand, supporters contended that the goal of Operation Choke Point was to shut down criminals, predators, and fraudsters. They argued that the allegations of a political motive were baseless and that the gun and ammunition documents were totally beside the point, part of long-standing FDIC best practices guidance and not related to Operation Choke Point at all.

What both proponents and critics of Operation Choke Point could agree on was that payment intermediaries wield tremendous power. Being able to be paid, by whom, and how define the terms of existence for organizations and people alike. In the metaphor of Operation Choke Point, money is like "air": those who are denied it can be "choked off."

Another striking illustration of the power of not getting paid came in 2010, when WikiLeaks began releasing thousands of classified US State Department diplomatic cables. A range of information intermediaries, seemingly in response to a memo by the Department of State, stopped providing services to WikiLeaks.[24] These included Amazon, which provided cloud storage, and EveryDNS, which hosted its website domain name. In addition, the accounts of the German foundation accepting donations for WikiLeaks were frozen by PayPal, Mastercard, Visa, and Bank of America.

As a *Wired* magazine blogger noted, there was an "element of theater" to WikiLeaks' struggles against censorship by its data and

domain-name service providers, because all of that information was mirrored elsewhere, including on more secure servers, but the attack on WikiLeaks' money flow was, in contrast, "the real deal and [had] the potential to genuinely impact the organization."[25] According to WikiLeaks, the payment embargo "blocked over 95% of our donations, costing tens of millions of dollars in lost revenue."[26] Indeed, the legal scholar Seth F. Kreimer points out that not being able to receive funds through payment intermediaries is perhaps the most effective form of "proxy censorship": it can actually shut down an organization.[27]

In today's "network society," power over the infrastructures that move around information, materials, or, in this case, value has become more potent than force, coercion, and other forms of overtly despotic power.[28] The stakes of not getting paid can be equally high even when there is no overt political agenda. If deprived of the "air" of payment, individuals and families can be "choked off" in the same way that Ponzi schemes and hacktivists can.

In 2015, there was a software "glitch" that resulted in thousands of reports of paychecks not being deposited by customers of the RushCard.[29] The RushCard, discussed in chapter 3, was started by the hip-hop mogul Russell Simmons and could be used to make payments and to receive direct deposits. The card wasn't linked to a bank account and didn't require a credit check or credit history; it was intended to provide financial services to those who would otherwise be "unbanked." Unlike many other prepaid cards, customers were encouraged to keep a kind of savings account by getting their paychecks direct deposited into their RushCard account. One customer complained on Twitter, "@rushcard it's been a whole week without money, it's hard out here. Single mother no help. I work hard for my money and now I can't get it."[30] Thousands of similar complaints are available through the Consumer Financial Protection Bureau's Consumer Complaint Database.

Then there is the case from one of my college students, whose Venmo account was recently suspended. He had purchased $400 worth of supplies for his fraternity's Super Bowl party. He was then paid back that $400 through Venmo by the fraternity's social chair, who added the caption "Super Bowl." The next day, he went out to

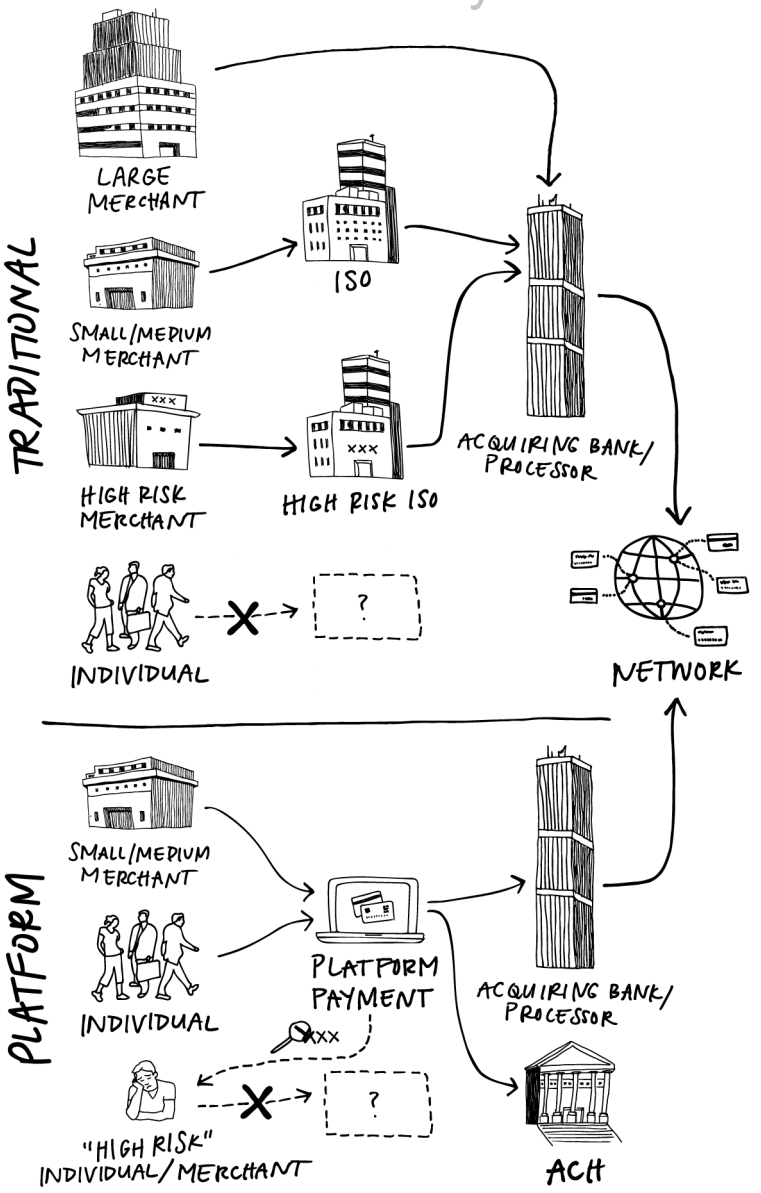
dinner with a friend and paid for his half of the meal through Venmo, adding the caption "Bet," a term that in current slang means "agreed" or "settled." According to the young man, his Venmo account was then frozen, with Venmo explaining that, between the large "Super Bowl" payment and the "Bet" payment, it had been flagged for gambling, an activity prohibited by terms of service. He said that he called Venmo and tried to explain, but his account remained closed, with some of his funds inaccessible. Everyone else in his fraternity uses Venmo, and most of their social transactions, both official and unofficial, are conducted through Venmo. Even as one of the most privileged members of our American society—a white, male student at an elite university—he is cut off from the dominant form of payment aligned with his transactional community, his communicative world.

To be a full member of any transactional community, to fully participate in a modern economy, and, indeed, to survive, you have to get paid. You have to have access to some kind of payment system, be it cash or electronic. And those systems have to work, reliably. A system that suddenly and unexpectedly cuts you off from money can be as perilous as not having access to any system at all.

Being able to get paid is perhaps *the* fundamental requirement for "citizenship" in a transactional community. Take the case of national currencies. It's fairly easy to be a tourist and use the local money to pay, but it's much harder to receive payments. This is often quite intentional: one of the myriad ways that boundaries and borders are invisibly enacted. Not being able to get paid means you don't quite belong.

Payment is communication, the transportation of information from one place to another. But money is, uniquely, information that is socially guaranteed to be valuable. It's the information that allows you to provide "operating expenses" for a business or for a family—to keep the heat on, to have enough to eat, and to pay your rent. Getting paid is an act of communication that can mean life or death.

But getting paid often goes unnoticed. In part, this is because getting paid is backgrounded, a predictable, regular beat in the



Getting paid with traditional and platform payment systems.

rhythm of our financial lives. For most people, getting paid happens less often than paying. Even those of us who live paycheck to paycheck mostly get paid, indeed, through paychecks, usually direct deposited into bank accounts. The problem is *usually* being able to earn enough money, not getting access to the money we have already earned. And yet when the systems we rely on to get paid stop working, the result is the same as not having earned enough money in the first place and can be devastating.

Getting people and businesses paid is an important part of the modern payments industry. Even for people in the industry, card payment "acquiring"—as discussed in chapter 3—is one of the least familiar aspects of the payments industry because there are many subtly different varieties in how it might be conducted.[31] There can be many layers, many middlemen, many different parties to your payment.

As described in chapter 3, merchants—or whoever is getting paid—pay to be paid. They pay their acquirer fees every time a card is swiped, as well as for information processing, leasing point-of-sale equipment, and so on. Acquirers themselves pay fees to credit card issuers for "providing" the customer. They then pass these fees along to merchants, plus additional markups for the services they provide. Card networks like Visa and Mastercard act as intermediaries between issuers and acquirers. They set rules and conduct payments by sending standardized messages between member banks, and they operate the computer networks that send these messages, as well as operating the information systems that process them.[32]

Large merchants usually connect directly to a large acquiring bank. Large merchants usually have internal teams tasked with managing payments and may even develop their own payments software, so they don't need as much information processing and other services as smaller merchants might. Smaller merchants usually don't connect directly to acquirers. Large acquirers—like JPMorgan Chase or Wells Fargo—don't typically provide merchant customer services, and small merchants don't bring enough scale to get competitive pricing. Instead, smaller merchants get paid through an independent sales organization, or ISO. ISOs are es-

sentially payment service wholesalers. They buy acquiring services in bulk from acquirers and then resell them to merchants.

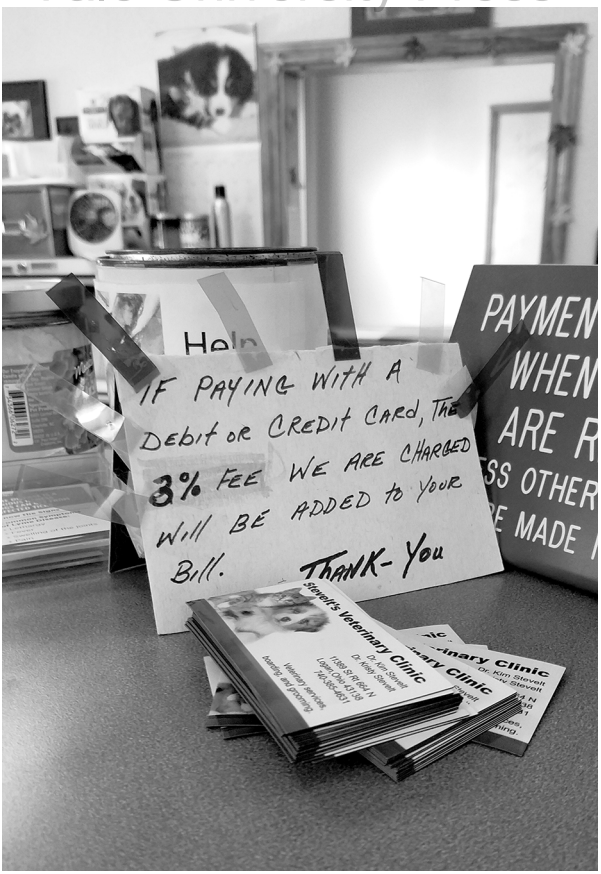
ISOs are often referred to as the "feet on the street" for the acquiring industry.[33] They provide ongoing customer service to merchants, such as data processing, software, and hardware like point-of-sale terminals. There is a lot of variability among ISOs. An ISO could be one person or a very large company. Some ISOs specialize in a particular industry or type of business. There can be multiple ISOs in between a merchant and the processor, each of whom gets a cut of the fees that the merchants pay. Pricing by ISOs is highly variable, depending on the merchant's industry and the kind of services the ISO provides.

So, when I buy a $2.10 coffee with my UVA Credit Union Visa card at a Starbucks first thing in the morning, it may seem like the money is moving only in one direction: my card issuer, UVA Credit Union, pays (via the Visa exchange system) JPMorgan Chase (which is Starbucks' acquiring bank); and JPMorgan Chase credits Starbucks with the money for my coffee.

But money also moves in the opposite direction: Starbucks pays a transaction fee to its acquiring bank, JPMorgan Chase.[34] JPMorgan Chase pays UVA Credit Union an interchange fee for supplying my business. Because Starbucks brings a high volume of transactions, it is charged relatively low, fixed rates. Starbucks has developed custom hardware and software to manage points of sale and has a variety of different internal corporate roles that ensure that it is able to be paid for the millions of cups of coffee it sells every day.

Conversely, it wouldn't make a lot of sense for my local independent coffee shop to do business with JPMorgan Chase directly. Instead, my regular café—let's call it C-Ville Joe—works with a small ISO—let's call it Commonwealth Merchant Solutions—that resells payments from Wells Fargo. The ISO does for my regular café many of the things that Starbucks' internal team does: manages point-of-sale equipment, ensures compliance to both legal and industry data standards, provides service when things go wrong.

In addition to selling payment services, acquirers also sell risk. When a merchant accepts a card payment, its acquirer temporarily



Sometimes merchants, like this veterinarian in Logan, Ohio, 2017, make the costs of card acquiring obvious to their customers.

fronts it the money paid. When I swipe my card for that cup of coffee, JPMorgan Chase effectively loans Starbucks $2.10, minus interchange, for my payment. Then UVA Credit Union settles with JPMorgan Chase for all the aggregated payments it owes. Finally, Chase bills me for that $2.10, along with all the other payments I made, plus interest.

If for some reason I dispute that $2.10 charge, citing fraud or dissatisfaction, UVA Credit Union initiates what is called a "charge-

back." When a chargeback occurs, the acquirer is responsible for refunding the money to the issuer, which in turn refunds the customer. Then, the issuer has to recoup that money from the merchant. UVA Credit Union gets that $2.10 back from JPMorgan Chase, which gets that money back—plus additional fees—from Starbucks. That liability travels through the food chain of acquiring. If I want my money back from C-Ville Joe, UVA Credit Union collects it from Wells Fargo, which collects it from Commonwealth Merchant Solutions, which collects it from C-Ville Joe. Part of the acquirer's job—part of the service it charges merchants for—is to "hold the risk" for the merchant. Every act of getting paid is also, temporarily, a loan.

Ideally, customers never want their money back, and if they do, merchants readily refund that money to their acquirers. In reality, however, it can be difficult for an acquirer to recover money from a merchant. For example, a merchant may face a cluster of chargebacks simply because its product is terrible, and it may go out of business for the same reason and be unable to repay its acquirer. And what about the case of actual fraud? The acquirer can try to recover that refunded money from the merchant, but if the merchant is a competent scammer, it will have already evaporated, leaving the acquirer holding the bag.

For acquirers, this risk is a business opportunity. ISOs serve as the middlemen for risk just as they serve as the middlemen between merchants and payment acquiring services. They take on the risk of the merchants they service for the acquirer. These merchants are sorted into risk categories: those that have a similar probability of chargebacks are priced similarly. Different ISOs have different "risk appetites." Some ISOs specialize in "high-risk" payments, and they charge merchants higher fees. The price of getting paid, in addition to scale, is tied to risk and, specifically, risk of chargeback. In the acquiring business, it is often said that "risk pays."

For ISOs that specialize in high-risk merchants, the ideal customer is one who is considered the riskiest—and therefore can be charged the highest prices—but who doesn't actually generate that many chargebacks and, crucially, is not actually doing anything illegal. In general, the industry standard for chargeback risk

is a 1 percent rate of chargeback transactions in relation to total sales transactions, and staying under 2 percent allows merchants to contract with a standard "high-risk" ISO; but risk—and the fees associated with higher risk of chargebacks—is highly variable.

Any legal merchant, no matter how "risky," can accept payment cards if it is able to find an ISO that will take it on—and if it is willing and able to pay the fees that the ISO sets. The ISO may ask the high-risk merchant to presecure the account, require personal financial guarantees from business owners, or implement other policies to mitigate loss. If a merchant has an increase in chargebacks, it is in the best interests of the ISO to put the merchant on an improvement plan or raise prices before cutting it off as a client.

Certain industries are categorically defined as high risk for chargebacks and outright fraud. These include those that sell products that are borderline illegal, such as counterfeit luxury goods and herbal drugs; those that are controlled in some states but not others, such as firearms; those that sell products that customers are likely to be unsatisfied with, such as psychic readings and get-rich-quick schemes; those that engage in deceptive marketing, such as diet pills and vacation time-shares; and those that sell products that customers might later be embarrassed to admit they ordered, such as pornography and gambling wagers. It's also common knowledge in the industry that chargebacks go up after the holidays, when consumers realize they've overspent. Whether rooted in embarrassment, regret, or just a desire to get something for nothing, this kind of chargeback is known as "friendly fraud," and it's built into the price of payment.

Acquirers can only go so far in charging high prices for risky business. In addition to managing risk, acquirers are also responsible for compliance with "know your customer" (KYC) regulations. This means verifying the identity of those on whose behalf they accept payments, demonstrating due diligence that these clients are not engaged in money laundering, funding terrorism, or otherwise engaged in illegal activity. If acquirers are found to be out of compliance, they can face heavy fines. In fact, the list of industries that so inflamed critics of Operation Choke Point was

really just long-standing guidance from the FDIC regarding due diligence for risk management and KYC regulations.

The notion of a "chargeback" demonstrates how payment is a technology used to manage risk. According to the sociological theorist Georg Simmel, modern money—that is, state-issued cash—allowed us to transact as strangers in the modern metropolis and to have an anonymous economy untethered from the bonds of family and patronage.[35] A key part of this is temporality of the transaction: in villages, exchanges were done mostly on credit, and everyone knew you were good for it because everyone knew where to find you; but in cities, you exchanged cash, and that was it. There was no need for a continued relationship. People getting paid didn't trust the person paying them, nor did they have to. They just had to trust in the cash. But cash, on its own, doesn't enable chargebacks. So, for those who exchanged their cash for goods or services, it was buyer beware. The card system, in allowing cardholders to revoke payment through chargeback, stretches out the temporality of the transaction. The card issuer becomes a guardian and a steward of the cardholder's financial interests.[36]

In recent decades, the acquiring business—the business of getting paid—has been changing in important ways. In the 1990s, high penetration of the World Wide Web promised a peer-to-peer economy, but there wasn't a way for people to pay each other using cards. The acquiring business was designed for merchants to get paid, not people. Payment cards were developed in the mid-twentieth century, for an economy that clearly delineated between buyers and sellers, and their design did not anticipate the geographically dispersed, person-to-person communication system and, crucially, economy of the internet era. Ordinary people aren't merchants, so they can't access acquirers the way merchants do. They don't have merchant services accounts, they can't be assessed for risk the way businesses are, and they aren't accustomed to paying high fees to be paid.

In the 1990s, new payments providers emerged with the goal of enabling people to receive payments from each other

electronically. These new systems were an overlay on existing infrastructure, a clever hack (or hasty kludge) that bridged old and new technologies and policies. The first and probably still the most successful service for people to get paid electronically was PayPal. The value proposition of PayPal, then as now, was to offer person-to-person payments in an online setting. In this context, there aren't clear "merchants" and "cardholders." Instead, there is parity between users, who sometimes buy and sometimes sell. In the industry, PayPal and other intermediaries like it are referred to as payment service providers, or PSPs.

In order to gain customers and make a profit, PayPal had to offer payment services at a lower rate than the existing payment system. This would have been difficult, if not impossible, in the traditional ISO model. PayPal would have been just another, additional middleman in the chain. PayPal's primary innovation, then, was to bypass the traditional acquiring system entirely. This newer approach to acquiring began with PayPal in the 1990s and continues to be the dominant model for emergent PSPs coming out of the tech industry, such as WePay, Square, Venmo (now owned by PayPal), and most payment systems embedded in social media platforms, such as Snapchat Snapcash and Facebook Messenger Payments.

PayPal bypasses the traditional acquiring system by keeping money inside its closed loop for as long as possible. When one user pays another through a PSP, the PSP records a transfer on its internal accounts, debiting the account of one user and crediting that of another. This is called a "book transfer." It is most advantageous to a PSP when the money never leaves the PSP's accounts and just goes continuously back and forth between users as book transfers. In this scenario, the PSP can charge fees of users without paying out fees to external systems. It can also make interest from the reserve of money held in users' accounts, or "float," as it's called in the payments industry.

When prompted by the user, the PSP uses a separate system to withdraw the funds from the paying user's checking account or credit card and deposit the funds into the receiving user's checking account. If a checking account is used, PSPs usually use the automated clearinghouse (ACH), a nonprofit network for bank-

to-bank transfers. The ACH, which was established by the Federal Reserve in 1975, was intended to function as a utility for financial institutions and charges very low fees. By riding the rails of the ACH, PSPs can avoid paying fees to the card networks, so PSPs encourage users to use their checking accounts.

If a credit card is used to fund the payment, PSPs enter the acquiring ecosystem not as an ISO but as a merchant that is operating on behalf of other small merchants. In the industry, this is called being an "aggregator" or "master merchant." As a master merchant, the payment service can then negotiate directly with the network, processor, or acquirer to receive custom, large-scale pricing, the same way a big box store would. It cuts out most of the middlemen, instead serving as the primary intermediary itself. When customers want to use their credit cards, PSPs usually pass the interchange fees onto them. Some PSPs are actually incorporated as ISOs, which means partnering with an acquirer, following particular rules, and meeting particular standards.

PSPs are often embedded inside a platform that facilitates marketplace transactions. For example, PayPal was a subsidiary of eBay for most of its existence, and while it can be used to pay in many different contexts, its initial function was to power the eBay economy. In the traditional ISO model, the interests of cardholders are represented by issuers, and the interests of merchants are represented by acquirers. In the platform model, the true client of the PSP is the platform, not the parties on either end of the transaction.

PSPs were originally envisioned as a way for people to get paid by other people when they couldn't contract with acquirers. Today, ISOs—seen as old-fashioned and overpriced—are a target for disruption by Silicon Valley. Traditional ISOs are rapidly losing ground to start-ups for merchant business as well. These payment-facilitation platforms might function like PSPs but also might be registered ISOs of a large acquiring bank. These offer an array of value-added merchant services, like loyalty points, analytics, and bookkeeping.

For a long time, ISOs were the only connection that small- and medium-sized merchants had to the card payments ecology. Like

most middlemen, they are frequently unpopular among their merchants and seen as price gougers. Today—at least in Charlottesville, Virginia, where I live—it's hard to find an independent coffee shop that uses a traditional ISO instead of a start-up. The tablet, equipped with software, a card reader, and a stylish swivel stand, is becoming more ubiquitous than the clunky point-of-sale terminal that ISOs lease to their clients.

The shift from traditional ISOs to start-ups has been accompanied by an important shift in the way that risk is managed. It is a shift in what sociologists call "riskwork"—the ordinary and mundane practices of imagining and managing risk—that produces payment failures for people like Eden Alexander and for college students with overly canny Venmo captions.[37] To manage payment is to manage risk, and to manage risk is a way of doing politics.

In the traditional acquiring system, there is a market for risk. Any legal merchant can get paid if it's willing to pay the rates

A traditional point-of-sale system next to a tablet with platform payment software.

commanded by a high-risk ISO. In new payment start-ups, risk is managed not through a market but through a mechanism native to tech-industry platforms: like other forms of social media, participation in these payment systems is governed by terms of service. Unlike traditional ISOs, which usually negotiate custom contracts with merchants, PSPs don't have direct vendor-client relationships with their users. Instead, all users are subject to the terms of service, which they agree to (but usually don't read) when they sign up for an account and which are subject to change at any time.

Transactions that would be considered "high risk" in the market model are simply banned. This is because PSPs access acquiring banks as master merchants, and in order to qualify for the lowest rates, PSPs must guarantee that all the transactions they conduct will be low risk for chargebacks. There are long-standing lists, provided by regulatory and industry groups, of high-risk merchant categories: time-shares, home-based charities, herbal remedies, and so on. Most payment start-ups simply take these lists and drop them into their terms of service as explicitly prohibited. Whereas in the traditional model, an acquirer had some sort of direct relationship and personalized contract with merchants, in the platform model, terms of service flatten these relations and, as the sociologist Robert Castel writes, "dissolve the notion of a *subject* or a concrete individual, and put in its place a combinatory of *factors*, the factors of risk."[38]

Like other social media platforms, these person-to-person payment systems use surveillance and automation to enforce these terms of service and to deal with the problem of risk. In addition to banning transactions that are considered "high risk," they increasingly use machine learning to monitor the social media presence of those who receive payments to catch such transactions as they happen.

PSPs that are designed for use by merchants, rather than people, are also governed by terms of service. Instead of merchants contracting with an ISO and paying fees tied to factors like their chargeback risk, they agree to the PSP's terms of service and pay a flat rate. For example, in the traditional model, a merchant who sells love spells would be charged higher fees by its ISO to cover

the risk of chargebacks from customers who find that the spell didn't beguile the object of their desire. In the new model, the sale of love spells would be banned entirely by terms of service. In fact, Square explicitly bans "occult materials." According to the founder of the Pagan Business Network, many of its members have grown weary of changing and inconsistently applied policies from PSPs and have instead sought out costly high-risk accounts with traditional ISOs.[39] Indeed, for the most part, traditional high-risk industries remain in the market model, accessing the payment networks through ISOs.

But this option—simply contracting with a high-risk ISO—isn't available to individuals, community groups, or other entities not incorporated as businesses. Neither the old nor the new model of acquiring was designed for "high-risk" categories of person-to-person or informal transactions. Face-to-face or online, people may try to use payment start-ups for purposes not approved by the terms of service, but they do so at their peril. They are likely to have their accounts frozen or even permanently suspended. Although PSPs endeavor to replace cash, they expressly prohibit the sort of flexibility that characterizes the person-to-person cash transaction. Because these policies provision who can receive payment, fundamental to participation in an economy and even survival, they are inherently political.

When Eden Alexander retweeted her supporters' offer of free pornographic pictures and videos to anyone who donated to her crowdfunding campaign, she unwittingly stepped into a gap produced by the misalignment of an older model of risk adopted by a new model of infrastructure. Unlike a traditional merchant, Alexander was not the client of the payment provider WePay; the crowdfunding platform GiveForward was.

Pornography, according to regulatory and industry guidance, is a "high-risk" industry. Merchants are subject to extra scrutiny because, it seems, transactions for pornography do present a high rate of chargebacks. According to some industry estimates, the rate of chargebacks in relation to total sales transactions for adult-services merchants can be as high as 4 percent. In comparison, a

low-risk business usually has a less than 1 percent rate of chargebacks in relation to total sales. It is widely accepted that people tend to ask for their money back for pornography. Some of these chargebacks are due to what payments-industry professionals refer to as "It wasn't me!" friendly fraud claims: because pornography is taboo, if purchases are discovered by a spouse or an employer, cardholders may be inclined to say that they did not authorize the transaction. Some of these chargebacks might be due to legitimate fraud. Perhaps also because pornography is taboo, many websites distributing pornography use deceptive tactics, such as misleading subscription pricing and spam. Pornographic sites have also been used as a trap to capture and illegally use credit card information.

So, in general, pornography is banned by terms of service from payment start-ups—including WePay—both for person-to-person payment and for merchant services. This industrial arrangement leaves out anyone who may not be able to develop a long-term relationship with an ISO, including individual pornographic performers. As Chris Mallick—who claims to have invented online payments when, in the 1990s, he started the first ISO that specialized in online pornography—put it, pornographers "had two jobs: taking pictures, and collecting cash. It turned out that they were really good at one of those things, and really bad at the other."[40] Mallick's vision of the "pornographer" as the one who "collects the cash" and "takes the pictures" rather than the person, say, who is *in* the picture is telling.

The systems of getting paid replicate long-standing imbalances of power within the sex industry: individual performers are imagined as commodities, not entrepreneurs, compelled to remain dependent on managers who have access to the infrastructure through which money flows. This usually takes the form of "payroll" checks from websites that have contracted with a high-risk ISO to receive payments or, of course, cash. While many industries have been radically changed by the internet's person-to-person economy, pornography—at least insofar as money and power are concentrated among middlemen managers—has not been one of them.

When Alexander was banned from getting paid, she wasn't just banned from receiving payments for pornography; she was banned from the system entirely. It wasn't just the donations that were motivated by the offer of pornography that were refunded—and, in fact, we have no way of knowing whether *any* donations were motivated by this offer. All the donations were refunded and the entire campaign was shut down. If Alexander had had another crowdfunding campaign, say, for a creative project, and had additional funds not related to the medical GiveForward campaign, she would probably have lost access to those funds as well.

During public uproar over the suspension of Alexander's crowdfunding campaign, the various platforms involved were eager to displace the blame. GiveForward blamed the terms of service of WePay. WePay blamed the policies of its payment processor, Vantiv. Risk was governed by a matryoshka doll of rules. Vantiv expects low-risk payments and therefore bans "high-risk" industries like pornography. This in turn determined WePay's terms of service, which in turn determined GiveForward's terms of service. Alexander agreed to all of this when she signed up for WePay. Whether or not Alexander was actually "selling" pornography and whether or not any chargebacks would have ever accrued became irrelevant.

People who happen to work in pornography, like anyone else, may seek to participate in online economic activity, but when terms of service are enforced by social media surveillance, the mere fact that they participate in the sex industry in ways evident on social media may be enough to exclude them entirely. It may be difficult for them to get paid at all: the ISOs exclude them from receiving payments because they are individuals, and PSPs exclude them because they are associated with high-risk industries.

The adoption of "high-risk" merchant categories by PSP terms of service, which are then surfaced and enforced by automation and machine learning, represents a misalignment of two different paradigms of risk and risk management. "High risk," as it was determined in the traditional acquiring model, was never meant to be a mechanism for exclusion. Rather, it was meant to create market categories for pricing. What was, as the sociologists

Marion Fourcade and Kieran Healy put it, a "within-market classification" used to create differential pricing becomes a "boundary classification" used to exclude certain transactions entirely.[41]

This moralized experience of payment is not limited to the moment of transaction itself. danah boyd has described how social media platforms often unintentionally create "context collapse," when one social domain suddenly comes crashing into another.[42] For example, neither my undergrad students nor I want to run into each other out on a Friday night, but if we become Facebook friends, we run the risk of seeing pictures of just those activities, which are clearly meant for an entirely different audience. A particularly dire context collapse occurs when the ability to get paid is lost because social media activity in one area of life (identity as a pornographic performer) crashes into another (crowdfunding for a medical emergency). These moments of context collapse make evident the problems of boundary classifications and the politics of risk management in payments.

In addition to agreeing to GiveForward's—and WePay's and Vantiv's—rules, Eden Alexander also agreed to be monitored for violations of these rules. Those terms of service were algorithmically enforced, and when Alexander hit that retweet button, she was caught in the dragnet.

Jillian C. York of the Electronic Frontier Foundation wrote on her Twitter account, "What someone does in their free time isn't [WePay's] business to monitor."[43] While porn was Alexander's job, not her "free time," York's point was that WePay's surveillance had unfairly conflated aspects of Alexander's life. She also tweeted, "Wow, do they follow me around SF too to make sure I don't accidentally strip?"[44] Instead of pornography being treated like a high-risk *transaction*, pornographic performers are being treated like high-risk *people*, even when they're not working.

In 2013, the year before Alexander's campaign, WePay launched Veda, an "intelligent social risk engine." Veda asks users for five pieces of information—first name, last name, name of business, email address, and phone number—and then uses its proprietary systems to mine additional data from social networks such as

Facebook, Twitter, and Yelp. Using algorithms, Veda analyzes "social signals" to measure risk and to make a decision about whether WePay will offer or continue to offer payment services. As WePay founder Bill Clerico put it, "Veda's intelligent brain is the new, smarter way to assess risk." Through Veda, WePay promised "no risk of fraud" through application of sophisticated machine-learning algorithms.[45]

In practice, WePay seemed to offer primarily increased detection of violations of terms of service by mining social media data for indicators of high-risk, prohibited behavior. Because WePay, like most PSPs, accessed its acquirer, Vantiv, as a master merchant, it was able to cite Veda as an innovative way to guarantee low-risk transactions and, therefore, undoubtedly lower its rates for transactions, which WePay was able to pass on to its platform clients, increasing scale of adoption, which would have no doubt pleased its venture-capital funders.

When Eden Alexander retweeted offers of pornography as an incentive for donating to her crowdfunding campaign, the transactions related to the campaign became, at least in the eyes of Veda, transactions for pornography. Even to GiveForward, a platform meant to mitigate the costs of health care, Alexander could not be treated with care but was, rather, as the legal scholar Pat O'Malley puts it, an "actuarial entity," statistically knowable, who had been surveilled and "diagnosed" with "risk," specifically risk for a chargeback that is unlikely to ever occur but nonetheless must be guarded against.[46]

Within the traditional payments industry, the important service that high-risk acquirers provide—and the substantial profits they can turn—are well understood. Vantiv, founded in 1971 as Fifth Third Bank, is one of largest and oldest merchant transaction acquiring processors, and it works with ISOs that serve numerous industries, including higher-risk merchants. Rather than blame Vantiv's "policies," it may have been more accurate for WePay to point to the specific contract that Vantiv had negotiated with WePay, which no doubt hinged on WePay's ability to guarantee low risk in terms of both chargeback and fraud.

Surveillance scholars have described how the power of surveillance lies not just in watching and recording but in identifying,

classifying, and assessing that which is surveilled.[47] Surveillance, then, is a form of "social sorting." As David Lyon writes, "Surveillance today sorts people into categories, assigning worth or risk, in ways that have real effects on their life-chances."[48] Payment systems like WePay work much like surveillance operations in the criminal justice system: they collect information to identify and classify individuals according to their risk of terrorism, criminality, or, in this case, violation of terms of service.[49] As Fourcade and Healy point out, the "classification situations" produced by the wrangling of "big data" are "presented, and experienced, as moralized systems of opportunities and just deserts." They "have learned to 'see' in a new way and are teaching us to see ourselves that way, too."[50] Indeed, when WePay froze Eden Alexander's account, it was one of the leading PSP start-ups that made extracting insights from social media data in order to manage risk its primary value proposition—and the basis for most of its venture-capital funding and ultimate acquisition by Chase in 2017.[51]

In theory, the tech industry should be keen to develop systems that, like ISOs, are able to profit from varied "risk appetites." Online lenders like Wonga, Lenddo, and Lendup are able to make loans—at high interest rates and other fees, most likely—to "digital subprime" borrowers, that is, borrowers who are, based on thousands of data points ranging from browser search history to Facebook friends, found to be at high risk of nonpayment.[52] But these probabilistic methods inherit a model of risk from an older model of payment, and they import it without adjusting it for a new context. Castel's description of the model of risk used to predict psychological deviance applies here: "A risk does not arise from the presence of particular precise danger embodied in a concrete individual or group. It is the effect of a combination of abstract *factors* which render more or less probable the occurrence of undesirable modes of behavior."[53]

In recent years, there has been a shift away from clear-cut risk categories in the payments acquiring business and toward probabilistic modeling and monitoring. While most platforms manage risk by applying blanket prohibitions of "high-risk" transactions, there is now a move to use data collection and machine learning

to model, identify, and control risk. But a shift away from lists of banned activities doesn't mean that account freezes have decreased or become less mysterious. In fact, there are countless examples of users unexpectedly not being able to get paid through leading person-to-person payment systems. Venmo accounts have been frozen over transaction descriptions that reference Cuban food, the name Ahmed, and weird jokes like "iced coffee obama nsa inside job syria," as well as actual donations to Syrian refugees.[54] Users have found that their accounts, and therefore their ability to receive funds, have been blocked when they try to raise money for charity, crowdfund without going through a crowdfunding platform, or receive an unusually large amount of money.

The shift away from clear-cut risk categories in the payments industry has come at the same time as the rise of predictive analytics in the tech industry. WePay, as we have seen, pivoted from being the "anti-PayPal" and the "unofficial payment system of Occupy Wall Street" to offering an "intelligent social risk engine" to "hit a moving target" in a world where "fraud doesn't stand still."[55] Predictive analytics systems, by their very nature, are always experimental. They are always being retrained to identity new attributes that correlate with unwanted risk—risk of chargebacks, risk of KYC violation—and to disregard attributes that do not correlate with these risks.

When Venmo accounts are suspended because of, say, using the term "Cuba" to annotate a transaction, users are told that they may have run afoul of the US Department of Treasury's Office of Foreign Assets Control and are asked to explain themselves.[56] In theory, every time a user submits an account of a night of drinking rum and coke or eating ham sandwiches or watching *Dirty Dancing 2: Havana Nights*, the system "learns" what not to flag. Eventually, it is hoped, Venmo's predictive analytics will get better at recognizing "real" violations and will no longer bother with these false positives.

These account freezes should not be seen as mistakes: they are evidence of the way machines learn, the way they are "supposed" to work. These systems—like most outputs of the tech industry—are allowed to live in "perpetual beta," in which products

are never really finished but are instead "developed in the open, with new features slipstreamed in on a monthly, weekly, or even daily basis."[57] While some kinds of "high-risk" transactional activities may no longer be overtly banned, surveillant systems may be less reliable because it is difficult for users to predict what kinds of transactions and activity—related or unrelated—will result in suspension of services. It's a question of how much "perpetual beta" users are willing—or are compelled—to tolerate.[58] Perpetual beta—to use the language of deconstructive democratic theory—creates a horizon of possibility in which machines are able to learn but not one in which humans are able to live.[59]

As risk-management systems have become more experimental, they have also become more opaque. WePay's Bill Clerico compared Veda's machine-learning capacities to credit scoring: "A traditional credit score only shows a sliver of who you are, but an online profile allows us to assign our users a more accurate 'WePay credit score' based on their personal history of verified, social data."[60] On the surface, a "WePay credit score" does not seem very different from a traditional credit score. They both use data points; WePay just uses more and different kinds of data. There is also a similarity with regard to how they are used for getting paid: an ISO uses a traditional credit score to price payment services for a merchant. But, again, a key difference lies in opacity and opportunity for recourse. The 1970 Fair Credit Reporting Act was intended to ensure that no secret databases were used to make decisions about Americans' financial lives and that Americans would have the right to see and challenge any such information.[61] No such regulations are in place for social media analytics.[62]

Nevertheless, variable risk remains incompatible with platform payments, where growth and scale often trump even profit and contractual relationships are governed by terms of service, which are blanket rather than bespoke.[63] The result is that some transactions—and some people—are banned entirely. Nowhere is this seen more clearly than in the adult-entertainment industry.

The "interlocking of intentionalities" and the challenges and failures of the payments industry to serve people working in

pornography reflect the larger set of interconnections among risk-management systems, governance by terms of service, surveillance-based business models, and access to economic infrastructure—conditions that may increasingly shape how we are all paid.[64] Any person who wants to get paid electronically is beholden to systems governed in ways that are inconsistently enforced, experimental, and opaque and offer little recourse for contestation.

Terms of service, across all kinds of platforms, tend to be inconsistently and confusingly enforced. This is no less true for platform payments. Kitty Stryker, in her blog post supporting Eden Alexander, noted several examples of successful GiveForward campaigns that seemed to directly violate WePay's terms of service.[65] WePay prohibits "weight-loss programs," but GiveForward had hosted a campaign to pay for someone to go to a weight-loss clinic and another for someone to have weight-loss surgery. WePay prohibits "magic, enchantment, sorcery, or other forms of yet-to-be-explained science," but GiveForward had hosted a campaign to accept "love gifts or love donations for psychic readings." WePay prohibits "hate, violence, racial intolerance, or the financial exploitation of a crime," but GiveForward had hosted a campaign that promised to reveal "the evils of the homosexual agenda."

Stryker's assertion that WePay was inconsistent at best and hypocritical at worst seemed confirmed when, less than six months after Alexander's campaign was closed, GoFundMe, another crowdfunding platform, partnered with WePay to host a campaign to support Darren Wilson, the Ferguson, Missouri, police officer who fatally shot the unarmed teenager Michael Brown.[66] Many people accused GoFundMe and WePay of violating their own terms of service, particularly the language about "hate, violence, racial intolerance, or the financial exploitation of a crime."[67] Backers of the campaign had posted statements like, "You deserve a medal, not a trial by jury" and "Thanks for giving that gorilla what he deserved."[68] Ultimately, the campaign raised $500,000 for Wilson.

There are perhaps reasons—which aren't totally obvious and don't necessarily make a lot of sense to the casual user of platform payments—that the campaign to benefit Darren Wilson was left open but the campaign to benefit Eden Alexander was closed. Fore-

most, no one offered racist materials to anyone who donated to the campaign, or, at least, no one organizing the campaign or benefiting from it retweeted such an offer. WePay did not respond to concerns about racist language on the campaign's page, but GoFundMe wrote a blog post defending itself against the "misinformation" surrounding the campaign. It argued that while there were many people on social media stating racist and hateful content in connection with the campaign, and even making comments on the GoFundMe page for the campaign itself, the organizers of the campaign were not responsible for the actions of others. Furthermore, the campaign's organizers had "repeatedly acknowledged and apologized for any offensive comments left by others and manually removed the comments from appearing on the campaign."[69]

WePay apparently draws very careful boundaries around what kinds of online behavior impact the transaction and violate terms of service. During the backlash following Alexander's account closure, a blog post from WePay claimed, "We have worked with other adult entertainers who use our service and abide by our terms of service without any issues."[70] A crowdfunding campaign may be supported by racists because they see it as a racist cause, but precisely when does the donation constitute a racist transaction?

In recent years, as racist groups have become bolder and sought to collect money for overtly racist goals, many have found that PSPs are unwilling to collect payments on their behalf. Hatreon—named as a portmanteau of the crowdfunding platform Patreon and the word "hate"—an explicitly alt-right crowdfunding platform, was embargoed by the card networks in 2017 before it could gain real any traction.[71] Cut off from payment, these racist groups have instead turned to Bitcoin wallets.[72]

As the internet researcher Tarleton Gillespie points out, platforms of all kinds routinely make these seemingly arbitrary calls about what is and is not acceptable, what does and does not violate terms of service.[73] The lines they draw are confusing and inconsistent. Racists and trolls are good at figuring out how to come right up to the edge of but not technically break a rule and knowing how and when to avail themselves of alternative systems. But for most people, including people who happen to be adult

entertainers, these lines are hard to walk. And it's harder than you might think to know what is and what is not "adult entertainment": in 2018, many platforms reclassified ASMR videos—in which performers, mostly women, whisper and make other sounds in order to trigger in listeners a tingling feeling, sort of like the opposite of nails on chalkboard—as pornography.[74] YouTube demonetized the videos, and PayPal blocked ASMR's practitioners. A failure to anticipate and, as the science and technology studies scholars Wendy Espeland and Michael Sauder put it, "react" to unpredictability is experienced as a moral injunction and a loss of access to payment.[75]

What happens when you fall on the wrong side of terms of service? Or are flagged by predictive systems as a violator or as an opportunity for a computer to learn? In the traditional model, merchants are the client of the acquirer, but in platform payment systems, there is often little means of recourse to users. While platform payment systems tend to offer more avenues for complaint than other social media services do, users usually face a byzantine and ineffective process, with little choice but to comply and wait.

One method that seems to be effective is public shaming of the offending companies. One blogger saw WePay's offer to restart Alexander's campaign as an offer "to make an exception for her, because people complained."[76] If Alexander had not been a popular member of a vocal and visible online community, WePay would probably not have felt the need to publicly offer her the opportunity to start her campaign over, and CrowdTilt would probably not have publicly stepped in to offer her assistance. As an MSNBC blogger wrote of another high-profile account freeze by PayPal, "If you ever find yourself under the thumb of a corporate monolith, make sure you have an army of Internet followers to back you up."[77]

At one point in the course of my research for this chapter, I was tweeting a lot about how hard it was for sex workers to get paid.[78] A representative from a feminist sex-worker organization direct messaged me to find out if I had suggestions for a payment system that her group could use to collect entrance-fee donations for its

annual conference. The representative explained to me that, on the one hand, she wanted to avoid companies that "actively discriminated against sex workers," but, even more importantly, her organization would be crippled if its account were suddenly frozen without timely recourse. She contacted several payment service providers and asked about what precisely would trigger a violation of terms of service. After all, she was organizing a conference *about* sex work, not paying or getting paid for sexual services. But she was considering paying honoraria to speakers, some of whom were sex workers. She didn't feel confident in any of the providers after hearing their answers.

And she had good reason to doubt any assurances. Indeed, there are plenty of stories from people in totally nonstigmatized situations: a blogger collecting money for Christmas toys for needy children and a game developer selling forum subscriptions that would finance completion of the game had contacted PayPal in advance, only to find that their accounts were frozen anyway.[79] Even as platforms embrace machine learning and automation in their fraud-detection strategies, sex work remains on the prohibited list. Indeed, in 2017, Gab, a social media platform popular among neo-Nazis for its lack of hate-speech moderation, was dropped by its payment processor, Stripe, for pornography.[80]

I struggled to give the organization representative a good answer. "Sexually oriented materials or services" are prohibited by the terms of service of most leading payment service providers, including PayPal, Square, Venmo, and Amazon Payments. Most of the payment service providers that are designed for use by sex workers aren't designed for individuals. For example, Verotel, one of the payment service providers cautiously suggested by the blog *Sex Worker Helpfuls*, specializes in payment processing for high-risk websites.[81] It is not clear how an individual sex worker, or a group organizing a conference, would be able to accept payments using it. Another company listed described itself as "the ultimate payroll solution for the adult entertainment industry" and was an e-wallet for managing paychecks from adult-entertainment companies. There seemed to be nothing that guaranteed reliable payments for sex workers.

It seems unlikely that the financial services industry will better serve sex workers anytime soon. In 2017, the End Banking for Human Traffickers Act passed the US House of Representatives and was introduced to the Senate by the strange bedfellows Marco Rubio and Elizabeth Warren. The legislation would, in a similar manner as Operation Choke Point, pressure banking and payment intermediaries to close accounts associated with suspected human traffickers.[82] Many advocates worry that such a law would do nothing to thwart "human trafficking" and instead would only hurt cam girls, porn performers, strippers, and other individual sex workers, making them even more vulnerable to an already unstable ecosystem.[83]

There were only two systems I could recommend to the woman with absolute certainty: cash and checks. Both, of course, were largely inappropriate for her purposes. It's unrealistic to expect a group to organize and promote a conference online, attract attendees from all over the world, but only accept donations and registration fees by mail. Paper payments alone—whether in the form of cash or check—simply can't move at the speed and geography of the internet era. They aren't able to keep pace with the way most of us live our lives today. The digital has become ordinary, and there seems to be no way for an independent individual also associated with the sex industry to *reliably* accept ordinary payments over digital channel, for any purpose. Porn performers and other sex workers have to choose between payment channels that are totally unreliable or totally inappropriate for the communicative reality and transactional community.

The technology of money has long tracked alongside the technologies that are used for communication more generally, and these technologies have created a shared geographic, temporal, and communicative lived experience: paper currency, like other forms of print culture, gathered people together under the auspices of the imagined community of the nation-state; postal expresses shipped currency and other forms of value alongside other forms of mail to further pull together far-flung regions into a communicative and economic whole; in the mid-twentieth century, electronic payment cards were part of an ecology of communication

technologies, such as teletype, the highway and personal automobile, and democratized jet travel, which enabled people to travel with greater ease.

Today, people communicate electronically, quickly and across great distances. Internet access, at least according to the United Nations, is a human right, but what about access to payment systems that operate at the speed and scale of the internet?[84] Our economies, like our communicative worlds, are electronic: We expect to text message our roommates and Venmo them rent. We expect to be able to get paid by a friend, relative, or employer in another state. In addition to access and reliability, a fully functional form of getting paid should also be aligned with the reasonable communicative expectations of our transactional community.

Plenty of Americans receive payments in cash, and while they are often assumed to be dodging paying taxes, they may also simply be availing themselves of the only payment system that is self-clearing, immediate, and truly reliable.[85] Cash can't get caught up, lost, or diverted by the infrastructure. Unlike company scrip, Walmart vouchers, or Amazon gift cards, cash is, as is printed on US dollars, "legal tender for all debts public and private." Cash may not be, as a Diners Club executive put it in 1963, sufficiently "modern" because it "can't keep up with the fast-moving world"; but it *works*, and it generally works for everyone.[86]

Getting paid becomes a bit more complicated when we try to develop systems for getting paid that both "keep up with the fast-moving world" *and* actually work, for everyone. Since the 1990s, payment professionals have dreamed and developed ways for people to get paid electronically, something that previously only merchants had been able to do. But we still haven't gotten it right, not for everyone and not all of the time. The task for those who hope to design how we get paid in the future is to figure out how to maintain all the things cash gets right.