Friday, 03-Mar-2006 16:05:07 PST
Post by former PayPal employee #1

I was a "middle management type" with Pay-Pal until leaving recently- partially due to my disgust over their internal security policies which have led to the mountain of complaints seen on this and other similar boards. There aren't many PP whistleblowers; during your "exit interview" a soon-to-be-former manager is warned, intimidated and threatened against doing the very thing I'm doing right now. But since I left to start my own business, there's not a thing they can do to me.

Pay-Pal DID start as an honest, legitimate company with an innovative service concept. However, in my opinion, this concept can never actually WORK in the real world because there are legions of scammers all over the globe with reams of stolen credit card info and identifications just WAITING to swoop down on any new "payment service" like this that comes along. Credit-card transactions where the "card is not present" and thus personally examined by a clerk account for the overwhelming majority of fraud transactions. Comparatively, there's very LITTLE credit card fraud at Wal-Mart, because the cashier actually sees both you and the card- and can ask for supporting identification at the point of sale. Unfortunately, the high-risk, "card not present" transactions are the ONLY kind of transaction a company like PP can do, and boy- did the con artists find them in a hurry! The basic con was (and is) to use stolen identification information to open new PP accounts, funnel money into them with stolen credit card numbers, then transfer the money OUT of the account before PP gets the charge-back and can freeze it. Unfortunately, despite PP's claims of having a "tough anti-fraud program", these people are mostly impossible to catch, because when opening a new PP account, they DO have all the proper-appearing ID information (which was stolen or conned out of unsuspecting individuals, most of whom have never HEARD of Pay-Pal). When fraud is uncovered and the account is checked out, the perp is almost never caught, since it was almost always opened under a stolen identity, and he's long abandoned the mail-drop.

Yes, the application process COULD be made more stringent, but it is felt (probably correctly) that a brand-new customer would certainly balk at doing things like sending in notarized copies of their driver's license and so forth. So an "alternate strategy" for offsetting the charge-back losses slowly evolved at PP. It's the perfect scheme really; since PP can't usually catch the scammers and doesn’t want to loose customer base by making things more stringent to start with- they decided to simply re-coup their chargebacks from the pockets (and accounts) of good, solid people under the easily-defensible and impossible-to-criticize guise of "Fraud Prevention and Enforcement".. Simply put, if you're a seller and somebody pays you with a stolen credit card, you're targeted by PP security and might very well have your account seized, "investigated", closed- and the money retained by PP. (Yes... they simply "add" it to their revenues and spend it like any other income. You basically gave them permission to do this under the "terms and conditions" you originally agreed to. No, I KNOW you didn't really read it, but I bet you will the next time!). Even if the person paying you has NOT used a stolen credit card, he could have been flagged by PP as "somebody to keep an eye on" for any

one of numerous reasons. If he does business with YOU, especially multiple times- you're frozen. OCCASIONALLY some lucky soul will complain about the seizure, and when the case is "investigated" by PP he is "cleared" and the money unfrozen. This good fortune has nothing to do with an actual "investigation" (there aren't any, really). Pay-Pal WILL unfreeze a small percentage of the accounts (as a future defense against a potential class action), so you MAY benefit from a simple luck of the draw. See, if it ever comes down to a massive class-action lawsuit, or even testimony before the SEC or other regulatory body, PP wants to be able to stand up in court and say "But your honor, we DON'T just freeze accounts and pocket the money. We really DO perform a painstaking investigation. Here's the proof... look at all these people who WERE suspected, but were then cleared by our "crack security staff"! If this was really a scam, why would we have given all of THIS money back?"

I'm amused by the posts that say, "But I've been a good customer of PP since the beginning and have paid thousands in fees.... why would they have done this to ME?" Let me answer that with a hypothetical question: If you were an unregulated financial services company so embittered by fraud losses that you, yourself, had completely lost whatever moral compass you might have once possessed, what would YOU rather have: a happy, content customer who's business might account for $5000 worth of fees over the next 10 years, or a person who's pissed off and will NEVER do business with you again, BUT you've got his $5000 up-front, TODAY- seized directly out of his account with no appeal possible. Believe me, it's a no-brainer to these people. They have sort of developed a weird corporate mindset wherein their past (and ongoing) victimization at the hands of con-artists somehow gives them license to "pass it along" to others. Think the E-Bay purchase will make it all better? Guess again. If ANY company knows the reality of on-line schemes and scams, it's E-Bay. While they certainly know that a nice chunk of their fees come from people who ultimately turn out to be thieves (but hey... their money is just as green as that of the honest folks) do you think E-Bay wants to open THEMSELVES (or a subsidiary company) up to the same risks as their bidders are exposed to? No way.

On another issue, I see lots of complaints from those who have BOUGHT things and paid through PP who find their credit cards suddenly drained and/ or billed multiple times for the same transaction. The answer is simple; PP has very lax hiring procedures, ESPECIALLY compared to the standards any bank would impose on anybody employed in a similar position of trust. But don't forget- PP ISN'T a bank, so they feel no obligation to hire (and, of course, compensate) people as if they were. Unlike the "account freezing" thing, the scams pulled on buyer's credit cards aren't a part of any "master plan" by the company, but simply the work of some dishonest employees who nonetheless have access to ALL of a customer's personal information. Yes, it's scary. Schemes are rampant where a PP employee has a cousin or friend set up an account to receive payments in another name. Since it's an "inside job", these "phantoms" will, of course, sail through the PP application process with flying colors- even if all of the information was simply "made up". Then your easily-accessible credit card number is used as payment for phony "auctions" and so forth done through the phantom account. The PP employee who actually approves this transaction might very be the one running the scheme! Given their

system and the way the computers are networked together, this is pretty simple for almost any employee to do. Even if you DON'T have access to the PP customer database, you almost certainly have lunch in the break room or visit at the water cooler with someone who does. Many people have been quietly terminated for this (rarely, if ever prosecuted- since this would be a huge black eye for the company), and in reality, THIS is where the majority of PP security and investigative resources go: to policing their shoddily-selected workforce.

So, if you STILL want to use PP- here are a few tips for merchants to avoid being taken by them. But really; from a moral and ethical point of view- would any decent person want to be in a position of supporting this ongoing Ponzi scheme- even if it COULD be guaranteed that you personally wouldn't be ripped off by it?

- Give PP only ONE account to access, then make sure that the monies are cleaned out the moment deposited funds become available- and transferred to an account that PP can't touch.
- After somebody has paid you through PP, NEVER do business with that individual a SECOND time- at least not through Pay Pal. This is a huge red flag to them, since scammers who get hold of a good credit card number but don't know the spending limit will "hammer" it through the same PP account several times until it's maxed. Don't forget- they're looking for ANY remote justification for seizing your money- since under the "terms and conditions" you agreed that this was OK with you.
- Never, ever, do business with anybody from Asia or Africa. ESPECIALLY Nigeria. With PP "security", you're venturing onto slippery ice even if you deal with a bona-fide American with an African or Asian sounding name. No kidding. I don't mean to sound like a racist here- but that's simply the way it is: an automatic "guilty until proven innocent" red flag.
- If you ARE frozen, accept the reality that this isn't some mistake that can be corrected by an e-mail or phone call to a nice customer service person; you've been SCREWED, and it's NO accident or misunderstanding. This company is now your enemy and is probably not inclined to do anything to help you, unless you're one of those unfrozen for "show" purposed as described above- but I'll bet they don't even account for 2%. So don't waste your time with "customer-no-service" e-mails and phone calls. Yes, most of the contact numbers listed on this site are accurate and the people listed are real employees- but believe me; they generally have NO power to say anything but "NO." If you've been frozen, your "case" goes to a special group within "customer service" who's entire mission statement could be summed up as "we've got the money, we're going to keep the money, so explain this to the customer in any plausible fashion- as long as the final answer remains "we get to keep the money'." Also, these folks will often be extremely rude to you- which is all part of the plan; you weren't really supposed to call them in the first place, and they don't want you to even THINK about calling back. Those repeated requests for copies of driver’s licenses and so forth are simply a ruse and a stall tactic. Believe me... they KNOW who you are, and this information does NOT keep getting misplaced. They're wearing you down,

> and it usually works. By the THIRD request for you to gather and send the same information, they most people will simply give up and say "it's not worth it." Don't threaten to sue or waste your money having a lawyer send PP a threatening letter, 'cause it doesn't work. People who SAY "I'm gonna sue" DON'T 99.9% of the time, and PP knows this. What DOES work is to hire an attorney and actually FILE SUIT. When they're hit with requests for discovery and are faced with having to send executives to depositions and so forth- most of the time your case will be "re-investigated". You'll then be cleared and your money will be returned. If that doesn't fix it, then, for some reason Pay-Pay must really, really feel that you ARE scamming. Most people simply won't go this far, since hiring an attorney, filing suit and so forth actually exceeds what PP has taken from you- and believe me, they DO know this.

For buyers the answer is real simple: NEVER use PP under any circumstances… EVER. You simply have NO control over who has access to your information, and your bank wouldn't touch some of these PP people with a ten-foot pole. Want to use a credit card to pay for an auction item but don't want to get double and/or fraudulently billed? Go down to the bank, use that same credit card to buy cashiers check, and then mail it to the seller. You have the exact same protection doing business that way as you do through Pay Pal, but you avoid the numerous risks of involving yourself with them- which, of course, go WAY beyond having to eat a thousand dollar loss because some guy didn't send your merchandise.

Looking for an alternate payment service? I can't honestly recommend one, since all of the others are prey to the same vultures that hit PP so hard. So I guess the system that works the best is one I'd simply call "pay, pal... "; you simply do business the old fashioned way: check out the seller as best you can, write a check and hope for the best- or simply deal locally. Given the realities and risks of "card not present" credit card transactions, I can't honestly see how any company who tries to do what Pay-Pal does could avoid becoming just like them, or else find themselves forced out of business under a mountain of chargebacks.

Any attorney who has a pending class-action suit against Pay-Pal and could benefit from my testimony can contact me at: expay-palguy@wildmail.com. Similarly, I'd love to hear from any former Pay-Pal managers who also feel morally obligated to "come out of the closet". I KNOW you know what this company is all about- and perhaps it's time we did the right thing by the people we unwittingly helped them loot. It would help me sleep better at night- how about you? Sorry, as much as I feel for you individual victims, I won't deal with individual court actions against PP- as to do so would doubtlessly consume ALL of my time, since there are so many. Similarly, I also can't intervene with the company on behalf of somebody who has been wronged. Follow my suggestion for getting your account unfrozen, and that would truly be your best shot.

~~~~~~~~~~~~

Ex Pay-Pal manager
~~~~~~~~~~~~

Originally posted:
http://www.paypalsucks.com/forums/showthread.php?fid=6&tid=1529&old_block=0