

## Heartland Payment Systems Attempts To Hide Largest Data Breach In History Behind Inauguration

Written by [rmogull](#) | Filed under [Cybercrime](#), [Non-Geek](#) | 52 comments

Brian Krebs of the Washington Post dropped me a line this morning on a new article he posted. [Heartland Payment Systems](#), a credit card processor, announced today, January 20th, that up to 100 Million credit cards may have been disclosed in what is likely the largest data breach in history. From Brian's article:

*Baldwin said 40 percent of transactions the company processes are from small to mid-sized restaurants across the country. He declined to name any well-known establishments or retail clients that may have been affected by the breach. Heartland called U.S. Secret Service and hired two breach forensics teams to investigate. But Baldwin said it wasn't until last week that investigators uncovered the source of the breach: A piece of malicious software planted on the company's payment processing network that recorded payment card data as it was being sent for processing to Heartland by thousands of the company's retail clients.*

...

*"The transactional data crossing our platform, in terms of magnitude... is about 100 million transactions a month," Baldwin said. "At this point, though, we don't know the magnitude of what was grabbed."*

I want you to roll that number around on your tongue a little bit. **\*100 Million transactions per month\***. I suppose I'd try to hide behind one of the most historic events in the last 50 years if I were in their shoes.

*"Due to legal reviews, discussions with some of the players involved, we couldn't get it together and signed off on until today," Baldwin said. "We considered holding back another day, but felt in the interests of transparency we wanted to get this information out to cardholders as soon as possible, recognizing of course that this is not an ideal day from the perspective of visibility."*

In a short IM conversation Brian mentioned he called the Secret Service today for a comment, and was informed they were a little busy.

We'll talk more once we know more details, but this is becoming a more common vector for attack, and by our estimates is the most common vector of massive breaches. TJX, Hannaford, and Cardsystems, three of the largest previous breaches, all involved installing malicious software on internal networks to sniff cardholder data and export it.

This was also another case that was discovered by initially detecting fraud in the system that was traced back to the origin, rather than through their own internal security controls.

-rich

### Posted on January 20

[Save to del.icio.us](#) (1 save) • [Digg This!](#) (5 Diggs) • [Email this](#)

## 52 comments

Dave Hull Jan 20

Any word on whether or not they were PCI Compliant according to some QSA(tm)?

LonerVamp Jan 20

Ghastly, just ghastly. And yet, for as much as we all could learn and improve from this

## Contact

Email: [rmogull@securosis.com](mailto:rmogull@securosis.com)

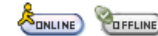
Twitter: [rmogull](#)

## Projects and Papers

[Understanding and Selecting a DLP Solution](#)  
[ipfw Ruleset](#)  
[Understanding and Selecting a DAM Solution](#)

## Search

## LiveChat

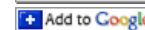


[mutube](#) » IM Online

## SANS Affiliate

[Sign up here for SANS Training](#)

### RSS Feed



## Subscribe

Enter your email address:

## Blogroll

- [Amrit Williams' Techbuddha](#)
- [An Information Security Place](#)
- [Chris Hoff](#)
- [DCS Security](#)
- [Emergent Chaos](#)
- [Errata Security](#)
- [Extra Pepperoni](#)
- [George Ou, ZDNet](#)
- [Matasano Security](#)
- [Mike Rothman's Security Incite](#)
- [Network Security Blog](#)
- [Network Security Podcast](#)
- [Rob Newby](#)
- [Security Ripcord](#)
- [South Pole Dispatch](#)

---

incident and any mistakes that led to it, we'll likely never hear the real stories.

All

[Still Secure After All These Years](#)  
[The Converging Network Threat Chaos](#)  
[ts/sci security](#)

---

rmogull Jan 20

@Dave- I suspect they would HAVE to be compliant, since they are a level 1.

content on this site is copyrighted under the Creative Commons Attribution License, Non-Commercial. Content may be reused for non-commercial purposes as long as it references this site.

---

Marcin Jan 20

@Dave Hull

[http://74.125.47.132/search?](http://74.125.47.132/search?q=cache:CRQ9ty_Bo3oJ:www.jobfox.com/Web/Seeker/WorkSampleFileHandler.ashx)

[q=cache:CRQ9ty\\_Bo3oJ:www.jobfox.com/Web/Seeker/WorkSampleFileHandler.ashx](http://74.125.47.132/search?q=cache:CRQ9ty_Bo3oJ:www.jobfox.com/Web/Seeker/WorkSampleFileHandler.ashx)

TrustWave?

---

Chris Pepper Jan 20

You guys are falling down on the job. It must be the miasma of hope & optimism disarming your natural cynicism. "began receiving fraudulent activity reports late last year from MasterCard and Visa on cards that had all been used at merchants which rely on Heartland to process payments." But he then says "In this case, the amount of information we know they did not get is long enough that except in very circumscribed cases identity theft is just not possible. At the same time, we recognize and feel badly about the inconvenience this is going to cause consumers."

So he's clearly lying.

They announced today to take advantage of distraction. They're not doing anything about fraud monitoring because it would be expensive and embarrassing. The bits about addresses and being safe are to cover their inadequate response and guilt.

---

Anonymous Jan 20

PCI compliance does not protect you against a targeted attack. It says you need to segment your transaction data from other networks. It says you need to control outbound rule sets. It does not specifically say how to do that or what is required during an audit.

---

Evan Schuman Jan 20

The contradictions in this case are worse than that. More importantly, it's unlikely these guys will be worse than TJX. (Not that it's a contest or anything.) If you look at the TJX numbers, it doesn't add up: <http://tinyurl.com/8onbf7>

---

Matt Harrigan Jan 20

Anonymous: the DSS is pretty ultra clear on using AV and anti-malware on all machines in the cardholder environment. I'd be willing to bet this wasnt occurring.

---

Anonymous69 Jan 21

@Matt Harrigan

AV ? "Anti-Malware" ? ROTFL!

you have no fsking idea do you?

htf would that make any difference?

---

Tim B Jan 21

I'm not sure where you are getting "100 million credit cards" from.

The Wired blog report indicates that Heartland learned of a potential breach in late October 2008. They eventually discovered the malware last week, in mid January 2009. So their systems were compromised for at least three months. If they process 100 million transactions a month, then that's a potential exposure of 300 million transactions. I suppose that assuming multiple card usage brings that down, but there's no mention of a guesstimated level of repeat usage in any of the reports I've seen of this so far.

Incidentally, Heartland were certified PCI-compliant in April last year. Given the time scale of October to January, that suggest that at least one quarterly review missed finding the compromise in their systems.

---

Anonymous Jan 21

@Anonymous69-

Thanks for the backup. Exactly. AV in its current incarnation is dead. The only way I have been able to correlate some of these 0-days is to look at behavior of outbound systems after a lot of whitelisting.

Anyone worth their salt will tell you that if your info is that valuable it isn't hard to write a piece of malware JUST FOR YOU.

---

Tom Jan 21

I use these people to process my cards at my service station. To date I have had no complaints but I am changing companies for my customers sake. I would just like to know why I was never informed of this.

---

Anthony Johnson Jan 21

HAH. Hey Matt long time man! This is a rather interesting case eh? I would have expected that internal tools and reviews should have captured external bound packets from the CHD segment...imo. =) But of course that assumes mature internal controls beyond a simple fire and forget audit solution...

---

Stuart Ward Jan 21

Sounds like an inside job to me.

---

BankcardGuru Jan 21

This is no surprise considering HPS got their start in the bankcard industry by processing credit cards for pornographic websites.

---

Anonymous69 Jan 21

@Anonymous

forget AVs, there's "rent-a-coder" now.

nowadays money+web can do everything, it's like a fucking game:

.you can rent people to code your modules for you and pay them with stolen CC's

.you can get CC's from all sorts of places on the web (stores,hotels,etc)

.you can also just hack middle mans of the card industry

.you can rent CPU power from cloud computing with stolen CC's

CC's are like gold in WoW, you just mine them. Russian's wet dream ;)

man power, cpu power, etc, it's all on the web now lol!

---

Eirik Jan 21

I agree with the posters stating AV (i.e., signature-based only) tools are near worthless in protecting high-value targets such as payment processors. More on that here:

[http://www.securitynowblog.com/endpoint\\_security/secunia\\_report\\_signature-based\\_antivirus\\_misses\\_most\\_unknown\\_malware](http://www.securitynowblog.com/endpoint_security/secunia_report_signature-based_antivirus_misses_most_unknown_malware)

(other related posts there too)

It is not clear to me what machines were infected and hence what machines could sniff the transaction traffic. This might account for there being fewer than 100 million records per month compromised. But, I'm shooting in the dark here.

---

Matt Harrigan Jan 21

@Anonymous69: It's not surprising that you're anonymous ;).

I was pointing out that there is likely a gap in controls, since this is in fact a pci related breach.

And yes, Anti-Malware, as in software that analyzes the behavior of untrusted executables and attempts to prevent bad instructions from occurring.

@Anthony - Hey hey! I know.. IPS/IDS should have picked up on odd traffic too right? Furthermore, what about FIM? Did this magic malware never touch the filesystem?

---

Anonymous69 Jan 21

@Matt

"I'm anonymous" because I don't even work in the security industry anymore, I just don't care and don't believe in security at all (even outside IT). My name here would be pointless.

"software that analyzes the behavior of untrusted executables and attempts to prevent bad instructions"

you've chosen a good wording when you said attempts :)

I mean, how can you really distinguish evil behavior from good behavior? too a certain point this is mostly a race. if

they are smart enough or simple not stupid enough they'd blend in, remember this is a targeted attack :)

assuming you know a typical REAL WORLD card processor infrastructure, aren't there always technical gaps like with any other real world infrastructure? :)

---

Greg Evans Jan 21

Tom,

We specialize in petro on the Buypass network. Send me an email if you're interested in moving.

[g.evans@intrinsicms.com](mailto:g.evans@intrinsicms.com)

---

Matt Harrigan Jan 21

@Anonymous69

No software successfully achieves its objectives 100% of the time, because flawless code does not exist and hardware performance is too variable. "hello, world" will fail if you run it 10 million instances of it simultaneously on even a relatively fast machine.

On the contrary - distinguishing what is good traffic on the network or what is a good instruction passing through memory is, at a high level, trivial theory. Even shell traffic encapsulated in https is easy to spot. Implementing it in software is hard to do well, but only because there are alot of moving parts.

Presumably, if the compliance metrics were measured correctly, and the controls were in place, as was indicated on the MC SP list, then no - there wouldn't be any gaps in compliance.

Gaps in security are unavoidable, but I think you need to ask yourself - who was the assessor of record in the last 2/3 -major- breaches, and is it possible that there is a pattern here?

---

Bling Jan 21

Careful Matt...just because you use to work at the assessor doesn't mean they went to hell after you were let go.

---

Ted Jan 21

Is our credit card safe anywhere??? Technology is moving too fast and will probably be our demise one day.

---

Matt Harrigan Jan 21

@Bling - Seems that i've hit a sore point. :)

Based on your inaccurate/off topic commentary, I'm guessing Gymboree let out early today.  
66.6% and counting.

---

rmogull Jan 21

Watch the personal attacks- that and spam are the only things we will moderate.

---

renee1180 Jan 21

I worked there for many years...trust me...someone should really question the corners they've cut...and a much needed large investigation is needed...

Additionally...its not just cards. HPS processes checks, micropayments, etc. All on the same servers that were breached....

Got lots of friends that still work there...in development and IT...worked in development myself...there are a LOT of corners cut.

---

Anonymous69 Jan 21  
@Matt

That's all very pretty in theory. You do have to realize that the industry you work in is completely helpless to avoid targeted attacks as this break-in.

As you said, "Gaps in security are unavoidable" and my friend, I think this event counts as a security more than a compliance breach LOL.

btw, trivial theory distinguishing good traffic ? oh god, please tell me you know what's a covert channel!

---

Matt Harrigan Jan 21  
@Anonymous69

I used an example of a covert channel in my last post and then you asked if i've heard of one. I think we're done here.

---

LonerVamp Jan 21  
@renee: Any specifics that won't jeopardize your identity? Maybe something we can learn from? :)

---

Anonymous69 Jan 21  
@Matt

sure, I just skiped the bit where there's actually an IDS/IPS product that does wirespeed covert channel analysis LOL

no worry, i forgot for a minute that you're in the industry, as in, you have an agenda.

so, why did you leave the assessor anyway ?

@renee1180

thanks for the info, now the russians that read this blog know about it! be careful not to get fired bruv!

---

Anonymous1000 Jan 21  
Tuesday was about the Inaguration, Wednesday was about Obama's 1st day. They are not hiding anything. The US mainstream media is picking up on the big story, an African American President! Get real people!

---

Bling Jan 21  
@Matt  
It wasn't inaccurate, and definitely not off-topic (since you brought up the subject).

@renee  
If corners were cut, come with substance and examples, otherwise it just appears that your post cut corners.

Other posters and articles had this right all along...compliance definitely does not equal total security by any means. If PCI failed Heartland, does that mean SOX 404 did as well (they are a public company, right)? What about the numerous other 'security' and regulatory audits they must go through? Computing security requires much more diligence and devotion than any of these compliance audits/assessments provide.

As far as the article...who knows why they chose inauguration day; anything beyond that is speculation.

---

creditcardman Jan 21  
The real problem that HPS had is the same one that RBS WorldPay had. Their system is their own...speaks their own language..and so as a result, it is not outside monitored. RBS WorldPay had some potentially 1.5 million customers breached last month for the very same reason. The Big Platforms- TSYSGLOBAL and PTECH are rarely, if ever compromised, because they are not owned and operated from within. They are platforms regulated in a far different and more visible way. You will see others like this in the future who have become their own platform and invested in the "infrastructure" to handle all their own transactions.

---

---

Alf Jan 21

<http://idiotinc.com/stock-market/ceo-carr-dumps-15-million-of-his-heartland-payment-systems-stock/>

Well, considering the CEO has dumped \$15 million in stock in the last six months, there could be bigger implications here..

---

Anonymous Jan 21

@Renee1180:

"HPS processes checks, micropayments, etc. All on the same servers that were breached..."

That's not possible, PCI says these systems should be on separate servers, and that services cannot be co-mingled! HAHAHA!

It is very clear who has theoretical experience and who has operational experience from this series of comments.

Management talking about risk and not liking what they hear leads to risk that is lowered. Operations people with no recourse and cultures of fear and reprisal rule the day.

In the end, it IS an arms race, and management doesn't want to hear it. They want to buy "security in a box". They don't want to hear that they need an army of skilled analysts reviewing traffic logs all day, nor do they want to acknowledge that they may need new tools that cost several hundred thousand dollars every 2-4 years. One of the first things I learned doing security is that a new analyst is usually far better buying another box. When they do buy a box, they don't know what they are buying, because the intent is just fulfill some checklist.

---

Rafal Jan 21

Hi Rich & everyone...

I don't want to sound overly alarmist... but I get that this is a huge breach, malware was installed, etc, etc... but you guys are missing the point.

(from my entry: <http://preachsecurity.blogspot.com/2009/01/heartland-payment-systems-quick-point.html>)

For your consideration:

- \* 100,000,000 account records
- \* 3% fraud, guessing conservatively
- \* \$500/incident of fraud

$(100,000,000 \times 0.03) \times \$500 = \$1,500,000,000 \rightarrow \$1.5\text{Bn}$

So, guessing conservatively\* this is potentially a \$1.5Bn security incident... why is no one focusing on this?

---

Anonymous Jan 22

Anyone that has worked as a qsa I am sure isn't surprised that Trustwave was their assessor. They are the rubber stamp assessor and soooooo far in bed with the PCI council that it is a joke.

---

Max Jan 22

In my eyes, the interesting question is: How did such a large breach (assuming it was large) go unnoticed for several month.

Clandestinely introducing malicious software (firmware or even hardware) into a more or less well secured environment is not easy, but feasible, as it is a onetime effort.

Effectively hiding the sniffed data, perhaps covering several hundred million transactions, giving at least double digit MBs, takes a little more ingenuity, but can certainly be done without arousing too much suspicion. That is, if the attacker chose to store the data in the first place and did not rely on sending it out alone.

The hardest part of such an attack should be, getting the data out without anyone noticing. I don't know a lot about network security, but from the little I do know, I would guess that preventing and/or spotting unexpected traffic leaving the relevant segments should not be too difficult. So in this case, an IDS/IPS and a few skilled and experienced operators interpreting the myriad warnings should have been the best possible defence.

---

---

rmogull Jan 22

@Rafal- that's the part I'm most interested in. In TJX they were able to quantify a lot of the losses, and those came out in some of the lawsuits (in the \$50-100M range if I remember).

---

merchantgrl Jan 22

They were breached a while ago and they just happened to pick that day to finally announce it?

Several people have brought up the Trustwave audit of April 2008. To be compliant, they need 'REGULAR' testing.

[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)

Requirement 11: Regularly test security systems and processes. What was there schedule for testing? audits?

Rafal is right- the financial implications are huge. Given the magnitude, and the lack of information being released on their new 2008breach.com site, it makes you wonder.

---

Mark Jan 22

I found a bunch of unauthorized purchases on my account due to the result of this. I feel violated and I am very disappointed in a system I should trust. What makes it so bad is that they knew about this for a long time and chose to release this news on Inauguration Day of all days. I guess their reason behind this is because the story would get buried. I feel sorry for Heartland Payment Systems for the consequences they are going to have to serve because of this bad choice.

---

Rafal Jan 22

@rmogull: I'm going to want to see quantifiable losses based on fraud and dollar-lost due to fraud cases (where they actually have to pay a merchant...) because that'll add up to more than just law suits and compliance violation fines... as I did some basic math above and in my post - even if you estimate conservatively on the fraud/loss aspect you've talking at LEAST a Billion dollars... that's a capital B ... ouch. The \*only\* sane way to avoid that kind of loss is to cancel each and every card that they've issued, ever... and if they're working at processing 100MM transactions a day I can give a good estimate on the number of cards they're re-issuing at around 70MM... that's an incredible cost - not to mention the negative PR of having to give customers new cards and cancel their current ones, and then everyone calling in to their support centers to activate their cards. The costs here are staggering and will go well beyond what gets reported, obviously.

Email me directly if you'd like to continue the conversation... maybe we can find someone to feed us some actual data and write that up as a case-study others can use? It makes one hell of an argument for whatever tools/procedures security people want to implement :)

---

Rafal Jan 22

@Mark -I'd love to talk more if you're willing... contact me directly through my blog if you're interested.

---

MikeA Jan 22

@Rafal

Excuse me as I may have missed something or my math wrong, but you are quoting a base of 100,000,000 accounts - that's 100 million transactions right? at 3% fraud? \$500 per fraud.

From what I've been reading it's 100M trasactions \*a month\*. Over 3 (possibly more) months. Even taking into consideration multiple transactions from the same card, the base number of accounts could be much larger than that.

---

rmogull Jan 22

Estimating fraud like that is risky. For example, how much time did they have to perpetuate the fraud? How much per account? Even if they could snarf 1 B card numbers, there are limits in how quickly they can convert it to cash. Also, 100M transactions per month doesn't equal 100M individual cards per month- we don't know the overlap.

That said, I bet it's a really big number :)

---

rmogull Jan 23

I just deleted a comment from Danielle Sylvia from msimerchantservice (.com), where she pretended to be a happy customer recommending msi.

Danielle, what part of "security blog" did you not notice? Do you really think we'd fall for something so blatant? Jeez- you need to go back to scammer school or something, I \*never\* would have passed such a feeble attempt.

---

[Liquidmatrix Security Digest » Payment Processor Discloses Epic Breach](#)

[Heartland Payment Systems Breach | Payment Systems Blog](#)

[Network Security Podcast » Blog Archive » Network Security Podcast, Episode 135](#)

[Network Security Blog » Network Security Podcast, Episode 135](#)

[While nobody is looking... « Brian Ladd's Blog - Notes on Life](#)

[Inside the Firewall » Blog Archive » Massive data breach at Heartland Payment Systems](#)

## Leave a reply

Name

Mail (will not be published)

Website

Notify me of followup comments via e-mail

## Related Posts

[The Breach Reporting Dillema](#)

[Things Not To Do If You're A Security Company](#)

[I Was Wrong. Sensitive Data \\*Does\\* Fall Off The Back Of Trucks](#)