Subject: Re: NYT article
From: "Peter Oppenheimer" Confidential
Received(Date): Fri, 16 Mar 2012 17:08:11 +0000
To: "Eric Gray" Confidential
Cc: "Dean Migchelbrink" Confidential "Eddy Cue" Confidential "Chris Keller" Confidential
Bcc: "Peter Oppenheimer" Confidential
Date: Fri, 16 Mar 2012 17:08:11 +0000

Dean,

Can you send something that shows for the last few months our write-offs for fraud that we are getting for charge backs and the level of refunds we are doing for customers.

Peter

Eric,

What would we need to do to provide better responses to developers? In thinking about this, we should not let this sentiment become fact by virtue of our not responding to developers, especially if we can demonstrate that this is not accurate. To the extent that it is, we need to fix it just as we did more than a year ago when ran into problems. This is very strategic to us, and we want to be bullet proof.

Peter

On Mar 15, 2012, at 9:47 PM, Eric Gray wrote:

Peter,

We've repeatedly answered this question and haven't yet identified a case where there is an actual issue. The perceived difference is always associated with developers who have significant levels of refunds and the associated timing of such refunds. Confidential

Confidential

In response to the point that we don't provide good support. We intentionally reply with a standard and rather vague response that the reporting is not intended to reconcile due to timing differences and we do not individually investigate each inquiry, but instead review enough of them to ensure both the daily / weekly reporting and the monthly financial reporting continue to be reliable for their intended purposes. We have good user guides and FAQ's that would allow one to reconcile things. Confidential

Confidential It never seem like a great investment, but we could re-consider.

I had heard from PR that this was coming, and it is unfortunate as the issue is very small as a percentage of our business and impacts a very small percentage of our developers.

We are making great progress on anti-fraud measures right now and have a very comprehensive strategy that we are in the early stages of executing on.

Thanks

Eric

On Mar 15, 2012, at 9:21 PM, Peter Oppenheimer wrote:

> Eric and Dean,
>
> This just posted from the New York Times. I know we are working on the customer account fraud points made in the article but I have not heard of the developer payment concerns below (which one cites in the millions). Here is the relevant section:
>
> One successful American game developer, who spoke on condition of anonymity for fear of retribution by Apple, said he started to notice discrepancies in payments last summer. The developer said his team had sent multiple e-mails to Apple, but that it had not addressed whether the missing payments were a result of fraud. Over the last year, the gap has amounted to millions of dollars, according to internal documents provided by the developer.
>
> With little action from Apple, some affected developers have banded together.

One Chinese developer, CocoaChina, has created an antifraud alliance of roughly a dozen developers.

While many of the affected consumers and developers said they did not blame Apple for their misfortunes, nearly all said the company could be more responsive, and noted that it lacked even a dedicated phone line to deal with complaints.

“Apple wants to pretend that everything is magic,” said Alex Stamos, co-founder of iSEC Partners, a security firm. “They need to admit that their products can be used by bad people to do bad things.”

What is going on here? Why are developer inquires not being answered?

Peter

For Apple, Pressure Builds Over App Store Fraud

By EVELYN M. RUSLI and BRIAN X. CHEN

In a little over an hour, Ryan Matthew Pierson racked up $437.71 in iTunes charges for virtual currency that he could use to buy guns, nightclubs and cars in iMobster, a populariPhone game. One problem: Mr. Pierson, a technology writer in Texas, has never played iMobster.

“This was fraud,” said Mr. Pierson, recalling the November incident. “I woke up, checked my e-mail, and I could see these purchases happening in real time.”

Mr. Pierson raised the issue with Apple and his bank, and the problem was eventually resolved. But his experience is hardly unique, as reflected by hundreds of online complaints saying that Apple’s iTunes Store, and in particular its App Store, which the company portrays as the safest of shopping environments, is not so secure.

The complaints come from consumers like Mr. Pierson, who say that their accounts have been hijacked or that some apps are

falsely advertised. And they come from creators of apps, who say they are having to deal with fraudulent purchases that drain their time and resources. Software makers also complain that competition in the App Store has become so brutal that many companies resort to artificially inflating their popularity rankings to grab attention.

It's a change for Apple, which was once criticized for its micromanaging of the App Store. Now the problem is not too much control, but too little.

"This kind of thing just happens any time a platform is successful," said David Edery, chief executive of Spry Fox, a small software company that sells games in the App Store. "People start flooding into it and it starts to get crazy."

The App Store offers more than 600,000 applications for iPhones, iPads and iPod Touches, and has already generated billions in revenue for Apple and

its developers. That makes it both the best deal going for software makers and consumers, and also a hulking target for those looking to manipulate the system and cheat people.

Apple declined a request for an interview, but said in a statement that it was working to enhance security. It advised customers whose payment information had been stolen to change their iTunes passwords and to contact their financial institutions.

In the shadowy world of hacking, it's often unclear how criminals get iTunes passwords or credit card information. But the App Store, and Apple's broader iTunes Store, have become playgrounds for illicit transactions. And the Web is rife with App Store scams. On Chinese online marketplaces, like Taobao or DHgate, some sellers are offering access to iTunes accounts for as little as $33. One seller on DHgate, for instance, has sold 56 iTunes

accounts for less than $35 each, promising thousands of dollars in "credit."

There are services that claim to generate codes for iTunes gift cards, and forums that explain how to use prepaid Visa cards to get free App Store purchases.

The scale of the problem is difficult to gauge without Apple's cooperation, though there is widespread anecdotal evidence, even on Apple's own site. On one Apple support forum, a thread titled "iTunes store account hacked," there are some 1,370 replies, starting in November 2010 and extending to Thursday. Last week, more than 100 people on Twitter who said they were iTunes users complained about stolen funds.

Last month, Daniel Saewitz, a 20-year-old Syracuse University student, was charged $81 for purchases related to a Chinese iPhone game. He alerted Apple and changed his iTunes password. But 24 hours

later, he said, his account was hacked again. In an e-mail, Apple said it was refunding Mr. Saewitz's money, but added that it was making an exception to its usual rules.

For developers, the scams can cause big headaches, eating up resources and damaging their reputations. Several game makers in China, where many of the hacks appear to originate, said they had lost hundreds of thousands of dollars because of fraud.

Hoolai Game, a Beijing-based developer that introduced an iPhone app last year, looked at its monthly payments from Apple and found that they were roughly 20 to 50 percent less than the sum of the daily reports it gets from the company. Hoolai and others say they believe these missing payments are fraudulent transactions that are wiped out by Apple.

More troubling for developers is that

consumers whose accounts have been improperly charged often blame the game makers. The reviews in the App Store for Kingdom Conquest, from the Japanese game giant Sega, include dozens from incensed users who accuse Sega of robbing them. Sega, which first noticed a burst of fraudulent transactions last summer, is still working on the problem, according to Ben Harborne, a brand manager at the company.

“We are very worried about reputation,” said Jian Huang, the president of Hoolai, who hopes to introduce a game in the United States later this year. “We have no way to tell the customer that we’re victims too.”

One successful American game developer, who spoke on condition of anonymity for fear of retribution by Apple, said he started to notice discrepancies in payments last summer. The developer said his team had

sent multiple e-mails to Apple, but that it had not addressed whether the missing payments were a result of fraud. Over the last year, the gap has amounted to millions of dollars, according to internal documents provided by the developer.

With little action from Apple, some affected developers have banded together. One Chinese developer, CocoaChina, has created an antifraud alliance of roughly a dozen developers.

While many of the affected consumers and developers said they did not blame Apple for their misfortunes, nearly all said the company could be more responsive, and noted that it lacked even a dedicated phone line to deal with complaints.

“Apple wants to pretend that everything is magic,” said Alex Stamos, co-founder of iSEC Partners, a security firm. “They need to admit that their products can be used by bad people to do bad things.”

One problem, Mr. Stamos said, is that iTunes customers use a single account and password to access all Apple services. For example, the same login can be used to download a $1 game or buy a $2,000 laptop through the Apple Store app. He said that Apple could adopt a two-step verification method like Google's. For example, if a user wanted to log in to the iTunes store on a new device, Apple could send a message to his iPhone containing a code, which he would enter to verify his identity.

Some App Store problems are the fault of the developers themselves — including those who make it harder for consumers to trust the store by cheating the system. The easiest ways to find new apps are Apple's Top 25 lists for different categories, including "most downloaded." But some of those downloads may not be generated by real people.

Walter Kaman, an independent programmer, said he was disheartened by a phone call from a service that offered to put his game in the Top 25. He said the promoter, whom he declined to name so as not to attract clients to the service, had hired someone to build an army of software "bots" that automatically download apps and drive up their rankings. The company wanted $5,000 for this service, said Mr. Kaman, who declined.

Mr. Edery of Spry Fox said his company was approached in October by a firm called GTekna, which offered to push its apps into the Top 25 for $10,000. Chang-Min Pak, GTekna's chief executive, said in an interview this week that it stopped offering such a service because Apple reminded developers in February that it was not allowed.

Then there are the customers who have been tricked into downloading apps that

are not what they seem to be. Apple has strict guidelines for developers, and it has tools and human reviewers to screen apps. But bad ones do slip through. One $2 app, for example, promises extra virtual coins for people playing the game DragonVale. But when customers download the app, no coins appear. The app has received dozens of one-star reviews from customers complaining that it is a scam and should be removed.

John Casasanta, owner of the iPhone app studio Tap Tap Tap, said the issue of developers manipulating the App Store remained largely unaddressed. “Apple has been doing the barest minimum to keep these things under control, because from their perspective, there’s simply not a problem,” Mr. Casasanta said.