Virtual Worlds 'Clear and Present Danger' for Money Laundering

April 26, 2007
By Brian Monroe

Print this Story

When Sony Online Entertainment executives discovered a computer user trying to move large amounts of money through one of its Internet-based role-playing games last year, they figured he was after more than some magical armor or an enchanted flaming sword.

They tracked down the gamer in Europe who admitted to laundering money through Sony's online universe – which allows players to buy and sell virtual goods with real money – by moving funds from a U.S. account to one in Russia, the executives said.

His defense: He said transferring money through the game was cheaper than using a bank, according to Sony officials, who wouldn't give further details about the case.

The threat of money laundering through virtual worlds—which give computer users anonymity and operate outside of government oversight—is real. Organized crime rings in Asia use them to defraud players and launder funds, said Julian Dibbell, author of *Play Money*, a 2006 book about his efforts to become a virtual mogul. Yet, there's little that financial institutions and law enforcement agencies can do to trace the origins of real dollars used to buy virtual goods online.

"It's the perfect crime," said Ken Rijock, a former attorney-turned-launderer and a financial crime consultant for World-Check. "It's a clear and present danger. There is no way law enforcement can even enforce the laws, because they don't apply."

Money Laundering Potential

Virtual worlds, which draw millions of users each year, are big business. One online game, Second Life, boasts a world populated by more than 5 million residents, or users. The virtual world has a daily cash flow of $265,000, a gross domestic product of $700 million and an economic impact of about $17 billion – akin to that of a small nation – according to the game's maker, San Francisco-based Linden Labs.

The game, launched in 2003, allows players to create digital versions of themselves – or avatars – and use their credit cards or an online payment broker like PayPal or Neteller to buy virtual currency called Linden dollars. Players use their Linden

to buy and sell houses, airplanes and virtual goods like dresses in online stores. Second Life gamers purchased more than $1 million in items in one 24-hour period, according to Linden Labs.

The growth of such virtual economies presents an opportunity for criminals, who can launder money by trading virtual property and converting profits from virtual cash to real currency, according to a report issued by consulting firm Deloitte in January.

Interpol, the international law enforcement organization based in Europe, said in an April report that criminals can take further advantage of online games with foreign exchanges that allow players to trade virtual currency like real-world money. The report said that “as a matter of urgency” law enforcement must learn how to investigate crimes involving virtual money and legislators must grant them power to recover data stored in jurisdictions where the crimes took place.

Easier Than Banks

Rijock, who laundered drug money in Miami in the 1980s, said it’s easier to cleanse funds through virtual worlds than banks, though banks are used at some point in the laundering cycle.

Here’s how it works: A drug dealer using fake IDs opens numerous virtual bank accounts through an online game. He deposits money into those virtual accounts through ATMs. The criminal’s online persona buys, say, virtual real estate from a co-conspirator – or even from one of his other accounts – and transfers payment to the seller’s virtual account. The seller can then convert the virtual currency into real money through a virtual money exchange and withdraw it from an ATM or a bank.

If investigators detect illegal activities in an online game, they must overcome a bevy of legal obstacles that make prosecutions difficult and embolden money launderers, Rijock said.

For instance, it’s unclear whether a U.S. federal court has jurisdiction over virtual crime or how an investigator can locate criminals who use fake names to create gaming accounts.

Impossible to Police

Gaming companies can’t police fantasy worlds because there “really aren’t any laws that govern what happens in them,” said Greg Short, director of Web presence for San Diego, California-based Sony Online Entertainment. “The legal system doesn’t extend here.”

Sony launched its first fantasy role-playing game, EverQuest, in 1999. In the game, players must earn gold and slay monsters to attain armor and weapons. Soon after the game’s creation, a black market spawned for players to buy video-game gold with their credit cards.

Sony didn’t allow these players to use such third parties. But, to cut down on fraud related to this black market, two years

ago Sony started its own currency exchange, Station Exchange. Although the exchange cut fraud in half in the first year, according to Sony, the company found that some gamers used it to launder money.

Short said the company checks the location of Internet addresses and holds Station Exchange transactions if investigators suspect fraud. Sony is considering switching to a more-secure system now offered by Visa and MasterCard that requires users to enter a code and identification information to conduct online credit card transactions.

“We are still figuring out the red flags … for laundering,” Short said. “Sometimes you have to learn the hard way.”

John Zdanowski, chief financial officer of Linden Labs, said there is “no indication anyone is using Second Life for money laundering or real-world terrorism.” Like online chat-rooms, these growing virtual worlds might interest law enforcement, but it’s “impractical for Linden Labs to police all in-world activities” itself, he said.

Banks at Risk

Still, the financial activity in virtual worlds is drawing the attention of Congress. Dan Miller, senior economist for the congressional Joint Economic Committee, is authoring a report on potential tax policy for online games and virtual worlds, which are growing at nearly 15 percent a month, according to Miller. The report, expected later this month, explores money laundering vulnerabilities and whether gamers should file tax documents when they make virtual profits or when those profits are converted into real money.

These worlds are “exploding … and just like any new medium of economic exchange, there are bound to be some people who try to exploit this,” Miller said. “It’s a new way to exchange economic value.”

The committee’s conclusions will help determine whether banks have to identify and monitor transactions that originated in virtual environments.

Banks already should be digging to see if transactions or accounts are tied to online worlds, said Ron King, head of anti-money laundering programs for Scotiabank in Toronto.

If investigators discover that a bank was caught in a virtual fraud scheme, the compliance team must document that they were “paying enough attention” and conducted due diligence.

The Unlawful Internet Gambling Enforcement Act, which took effect October 1, forbids financial institutions from knowingly accepting funds from Internet gambling operations. King said banks could be held responsible for processing virtual world transactions like they are for processing Internet gambling transactions.

Banks should not assume carte blanche that transactions from third-party payment processors are legitimate, he said. Instead, financial institutions should look for patterns that could reveal suspicious activity. “There’s a definite risk for banks.”

April 26, 2007
By Brian Monroe

Print this Story

212 661 1325 | InformCustomerService@Fortent.com

http://inform.fortent.com/FortentWeb/NewsSummaryHomeGuest.htm?GUID={fd2f1878-b1ba-4980-887e-157ceff6a3ba}