BY JOANNE CHRISTIE

For consumers, cyber crime is sometimes little more than an annoyance. A fraudster steals their card details, purchases something, they tell their bank, the money is refunded and the problem is sorted. An administrative hassle perhaps, but it's rarely fatal to their finances. For e-commerce businesses, however, that usually have to foot the bill for the chargebacks that occur following unauthorised card transactions, it's more than just a hassle. Identity theft, along with other forms of cyber crime, are serious issues that threaten online gaming company's reputations, bottom lines and, in some cases, their licence to operate. But just how big an issue cyber crime is for the online gaming sector is open to debate. The countless number of companies selling tools to combat cyber crime would have us believe we live in a world full of virtual criminals, while operators are understandably keen to play down the prevalence of anything untoward taking place.

Unauthorised card transactions and the resulting chargebacks are a continuing problem for the industry, though this is also true of e-commerce businesses, says Clive Hawkswood, chief executive at the Remote Gambling Association (RGA). "It's not that the level of chargeback fraud is rising disproportionate to our industry, it is just that as the industry has got bigger the annual figures have got bigger."

Advances in identity-verification tools and additional card security measures such as Verified by Visa and MasterCard's SecureCode have helped, but hurdles remain, says Dave Pope, marketing director at 192.com Business Services. "The challenge for the online gaming industry is that it wants to expand internationally – the UK is a very crowded marketplace – but it is more difficult to get hold of the data to verify identity outside the UK. So we can't offer as in-depth a verification service for Germany, France or Australia as we can in the UK."

One problem that seems to have gained less coverage in recent years – certainly when compared to the spate of attacks that were reported around five or six years ago – is denial of service (DoS) attacks. The online gaming industry was an early target for DoS hackers, but was quick to head off further extortion attempts with preventative measures. Emma Lindley, strategic development director at GB Group, says the hackers have moved on to easier targets. "Those attacks are still prevalent, but what we see now is because most of the mature gaming companies have had those

CONTINUE

"DATA RELEASED BY ANCHOR INTELLIGENCE IN JULY REVEALED THAT CLICK FRAUD ATTEMPTS HAVE INCREASED BY MORE THAN 25% IN THE PAST YEAR"

attacks early on, they've actually found ways of getting around them. What we do see is new entrants being hit."

Some issues are specific to certain games, for example collusion and money laundering are more prevalent in peer-to-peer games such as poker, where criminals have the opportunity to move money between cards by working with others.

Pat Harrison, operations director at 32Red, says: "Certainly when you talk about player collusion, for those operators that are specifically reliant on poker, then that is a big concern. Poker is one area that has to be more tightly policed because of the business model involved. There is a large police network set up to monitor game play to pick up any hints of soft play that would indicate that people are just trying to wash money through."

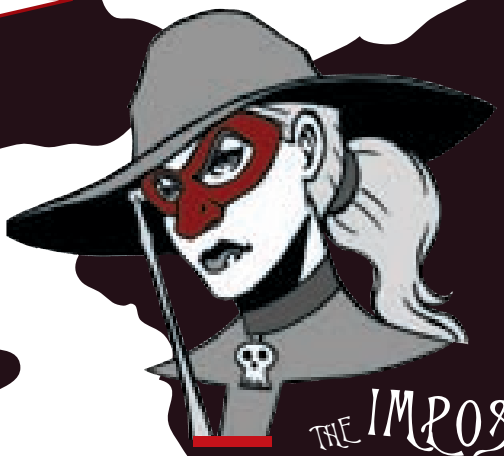
With savvy players ready to pounce on any hint of anything untoward – poker forums such as Two Plus Two have been largely responsible for breaking stories such as the Ultimate Bet cheating scandal – operators need to ensure game play is above board. Harrison says cheating scandals can affect the credibility of the industry more widely. "If people are seeing operator A being targeted, then people are hesitant about other operators," he says.

Data security is set to become one of the biggest issues the sector will need to tackle in coming years, says Lindley. "Fraud can be perpetrated externally and internally. Employee-type fraud has definitely increased. Criminal gangs will pay people large sums of money within call centres to let large transactions go through. They'll say 'we'll give you £10,000', and to somebody who earns £16,000 a year, that's going to make sense.

"We've also seen quite a lot of gaming companies now starting to carry out audits on us. They want to understand where their consumer data is going. That's one area I think they are going to start getting hotter on."

Data breaches and insider scandals of course also have the potential to turn into PR disasters. Media coverage, however, can be disproportionately harsh when it comes to the online gaming industry due to the lingering stigma attached to the sector. The

"IT'S NOT THAT THE LEVEL OF CHARGEBACK FRAUD IS RISING DISPROPORTIONATE TO OUR INDUSTRY. IT IS JUST THAT AS THE INDUSTRY HAS GOT BIGGER THE ANNUAL FIGURES HAVE GOT BIGGER"



THE IMPOSTER

As any teenager trying to buy alcohol will know, it's hard to fake your identity in person. It's much easier online, where enough knowledge of another person's details can see criminals gain access to their funds with just a few clicks. Chargebacks have long been a problem for the online gaming industry, and indeed e-commerce generally suffers a higher rate of fraudulent transactions than businesses with a physical presence. Although the latest figures from the UK Cards Association are encouraging, showing that year-on-year card-not-present fraud fell in 2009, the tight margins online gambling firms operate on mean it's vital they keep imposters at bay.

While more sophisticated identity-verification systems, coupled with the introduction of Verified by Visa and MasterCard's SecureCode have helped combat card fraud, imposters are continuously looking for, and finding, ways around even the most intelligent technology. Where a new player's identity cannot be verified, operators face a tough choice – take a risk or demand hard-copy proof of identity, which in an online environment, often turns even bona fide punters away.

Though many imposters are simply looking for a way to cash out by using stolen cards, some are simply looking to feed their gambling habits without incurring any risk and account takeovers are on the rise.

THE COLLUDER

Just as criminals have long tried to dupe land-based casinos by sitting at a table with two of their associates and sharing information about their hands with a wink or a cough, cyber fraudsters also try to manipulate game-play by cheating.

The colluder is most likely to be found at the virtual poker table, where the multi-player format lends itself better to collusion than single-player games or sports betting. Some cheats will simply aim to win money from other players – it's easy to gain the upper hand when you know what three of the players are holding – while others will combine collusion with other types of criminal behaviour such as money laundering or identity theft. Those trying to wash money or steal it from a card are likely to intentionally lose to another criminal, who will then cash-out the funds.

The financial cost to operators is high, as chargebacks are particularly pricey when they come from cards used by players who are betting with a different operator on the same network. Their customer base is also likely to suffer, as a reputation for tolerating cheats is likely to both turn away good customers and encourage more cheats.

Operators have a sophisticated variety of software tools at their disposal to identify incorrect betting patterns which can expose cheats, the majority of which adopt far stronger policing of poker games. Even so, two separate cheating rings – one involving bots and another Chinese players – have been uncovered on PokerStars this year alone.

The Money launderer

Speculation abounds that the online gaming industry is a haven for money laundering, but this can often be more rumour stalking the industry rather than fact and money launderers themselves. A report prepared for the Remote Gaming Association last year by MHA Consulting concluded there was little evidence to support the view the industry was particularly susceptible to money laundering or financing terrorism. This was said to be partly due to the lack of cash transactions and the combination of statutory and self-regulation present in the industry.

However, the potential to wash money through the system exists and operators with poker offerings, or that allow player-to-player transfers, are often at greater risk. Because operators generally return all winnings to the card of origin, money launderers are more likely to work with other criminals in order to benefit – possibly by chip dumping in order to transfer money from one card to another.

UK regulations place particularly onerous requirements on operators, requiring them to not just report any suspicious money-laundering activities, but also, because it has such a narrow definition of money laundering, to be aware of any attempt to spend or wager dirty money.

MRGA's Hawkswood cites underage gambling as a good example of an issue that is often blown out of proportion. "The reason it is always an issue is for PR reasons. If a newspaper does a story on it then the reputational damage is huge, even if in reality the numbers are very low."

Media perception aside, the majority of people agree online gaming is no more or less at risk from cyber criminals than any other online businesses. "The threat of criminals is present in all industries and across society, and it is important to recognise that the issues facing online gaming are not specific to this sector," says Kristoffer Cassel, head of AML and fraud prevention at Unibet. "What I believe differentiates this sector from many others is that we have been recognising these risks from the start and, since day one, worked with commitment in this area," he says.

"This self-regulation and commitment has been driven as much from the businesses as from licensing requirements. I wouldn't be surprised if in the future we see some of the high-street banks using systems developed from within the gaming industry," he adds.

Harrison concludes: "I think the sector is very much ahead of the game purely because the margins that gaming operators work to are miniscule and as a result of that then we've got to minimise any potential loss of hard-earned revenue."

The Hacker

Hackers target both operators and their customers. Their most damaging work takes the form of denial of service (DoS) attacks, in which hackers overload an operator's site – typically by infecting other computers using malware or botnets – to the point where it is so overwhelmed with traffic that it collapses. A spate of DoS attacks was perpetrated on gambling sites five years ago with many criminals forcing sites to temporarily shut down, as well as blackmailing operators, who were either forced to pay up or lose crucial revenues.

As an early target, the gaming industry was quick to adopt security systems aimed at preventing future attacks, with a number of companies designing products to help operators cope with hackers. While DoS attacks cannot be considered a thing of the past, many extortionists have moved onto less established operators, who they see as easier targets.

Hackers may also use botnets to carry out click-fraud using them to infect machines and drive up advertising costs for operators. Data released by Anchor Intelligence in July revealed that click-fraud attempts had increased by more than 25% over the past year.

Hackers also target punters themselves by directing them to fake websites via chatrooms within legitimate sites and enticing them to divulge personal details by offering hefty sign-up bonuses.

The Insider

It's often said that an organisation is only as strong as its weakest link and even with the proper due diligence, references and criminal checks, any employer can fall victim to a disgruntled employee.

Earlier this year, Ladbrokes faced a scandal when UK newspaper *The Mail on Sunday* reported that it had been given confidential records of 10,000 customer accounts from a person claiming to have previously worked for the company. A further 4.5 million accounts were then offered to the paper, however, it reported the incident to Ladbrokes and handed the files to the Information Commissioner's Office (ICO), Britain's data watchdog.

A white paper prepared by 192.com Business Services, *MO: The Fraudster's Modus Operandi*, found that fraudsters attempted to steal data from companies by both planting themselves as employees inside the organisation, and by targeting low-paid workers, such as call centre staff, and offering them large sums of money to hand over company data.

Not all perpetrators are badly paid however, as evidenced by the Ultimate Bet cheating scandal. In 2008 World Series of Poker champion Russ Hamilton, who had worked as a consultant for the company, was exposed as the main perpetrator of the cheating scandal that eventually cost the company more than $6m.

To ward off potential breaches, operators can employ security measures to ensure only a handful of employees are able to view full payment card details and have no way of recording the information.