› Point of View

Online Fraud: Increased Threats in a Real-Time World

Online fraud is increasingly seen as an urgent threat by banks across the world. According to industry body Financial Fraud Action UK (FFA UK), in the UK alone losses from online banking fraud rose by 48 percent in 2014 compared with the previous year[1], with a growing number of consumers conducting their financial affairs on the Internet. In addition, cybersecurity firm Kaspersky Lab[2] reported that Brazil has the largest number of users attacked by banking malware (a key modus operandi for online fraud) followed by Russia and then Germany. Moreover, a recent survey by Deloitte[3] indicated that most banking frauds in India occur within the retail banking sector.

With fraudsters capable of circumventing banks' existing authentication systems, the need for sophisticated analytics technology that enables investigators to take proactive action to eliminate online fraud at the source is becoming ever more acute.

With fraudsters capable of circumventing banks' existing authentication systems, the need for sophisticated analytics technology that enables investigators to take proactive action to eliminate online fraud at the source is becoming ever more acute.

[1] Kevin Peachey, BBC News Service, "Online banking fraud 'up by 48%'," .

[2] Huntrevenue Services, "razil leads the rankings in online banking fraud,".

[3] Business Standard, "Survey reveals rise in retail banking fraud,".

[4] Clare McDonald, ComputerWeekly.com, "Faster Payments plans to widen UK scheme,".

Urgent Attention Required

The move online is hugely positive for both financial institutions and their customers. Banks are using online payments as a first step in building a more coherent, holistic view of each customer. Moreover, with customers' growing preference for communicating through tablets, smartphones and other mobile devices, banks must continue to offer up new ways for them to interact with their accounts. The ongoing migration of the banks to faster payment mechanisms is a great example, where today's digitally demanding, fast-paced consumer expects to be able to make payments to any company, institution or person in real time, at any time and from any place. The Faster Payments scheme has been very successful in the UK[4] – and interest in this approach has now extended to other international markets.

The opportunities for enhancing customer service delivery by offering new service solutions, such as faster payments, are clear. However, digital channels are innately more vulnerable to fraud, and, while the speed and openness of the approach make banking faster and more convenient for customers, it can also make it easier for fraudsters to access money and transfer it quickly without being detected until after the crime.

Put simply, online channels help criminals remain hidden and anonymous. When customers apply for lending online, or make a payment via their smartphones, banks have less understanding of who is truly behind those activities than in the past when face-to-face meetings were more typical.

sas
THE POWER TO KNOW®

It's a problem they need to tackle urgently, with both individuals and businesses potentially losing thousands in a single attack. The overall financial losses can be huge, and – when combined with the significant impact of reputational damage – the serious consequences of this type of fraud are clear. Earlier this year, for example, details emerged in the national news of the decision of a business owner in Australia to sue the Commonwealth Bank, arguing that security flaws in its online banking website allowed one of her employees to steal more than AUD 1.1 million (US$847,000).[5]

Under Attack

The drivers for committing this crime are varied – but there are currently "perfect storm" conditions in place, with the move online combining with an increasingly tech-savvy generation, continuing economic uncertainty and a lack of controls creating fertile conditions for fraudulent behavior.

And the increasing capability of the fraudsters is reflected in the growing variety of methods in use. Among the most prevalent are phishing – when fraudsters send emails impersonating legitimate companies to lure recipients into revealing confidential information – and its variant, vishing, a form of voice phishing requiring the intended victim to respond by telephone to an email or phone message. These techniques, which are increasingly widespread, often target the most vulnerable within our society, including the elderly, who are likely to be less aware of this type of threat.

Malware, malicious software designed to disrupt the performance of PCs, laptops or handheld devices, is also ubiquitous – with schemes becoming so well executed that it can be almost impossible for users to recognize that their devices have been infected.

Money mules, people who are both knowingly and sometimes unknowingly recruited by fraudsters to transfer money acquired illegally, also contribute to the success of many online banking frauds. Indeed, we see many instances of fraudsters obtaining key account password and login details to gain access to victims' savings accounts, transferring huge sums into current accounts and then using mules operating at ATMs to drain these accounts within minutes.

The lack of a consistent pattern to this fraudulent activity makes it even more challenging for the authorities to analyze. Banks can be attacked repeatedly for a period of time and then react by putting new controls in place to deter the fraudsters, causing activity to then typically drop away, only to return months later once the fraudsters have developed new techniques to bypass the controls.

While offering a diverse portfolio of financial products, in an environment where the fraud is fast-paced and forever changing, most banks have little in the way of viable technology to provide the much-needed protection. Indeed today they are often overly reliant on authentication systems that provide unambiguous identification of users through a combination of components known only to that user – such as user names, passwords, bank codes or PINs.

Banks often believe that this type of approach is sufficient in itself because historically it would have been largely effective. Yet with new fraud threats emerging all the time, that is no longer the case. As a result, the battle is currently being played out in the criminals' favor, with the fraudsters innovating faster than the banks.

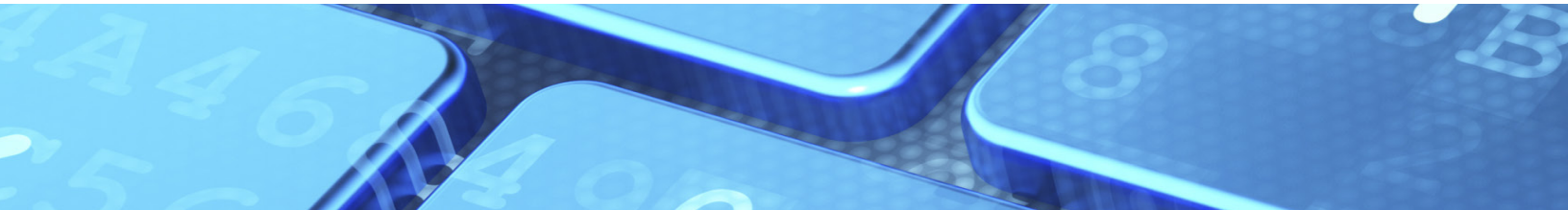
End-to-End Protection

Clearly banks must take a more sophisticated approach to online fraud detection and be in a state of constant readiness.

Careful data monitoring and management is critical from the outset, and banks must, where necessary, enhance their data quality and be able to collate and link together the wide range of different data types ingested into an organization, including financial and non-financial transactions, customer information, bank account details, computer IP addresses, and information about devices and their usage patterns.

> The overall financial losses from online fraud can be huge and, when combined with the significant impact of reputational damage, the serious consequences of this type of fraud are clear.

[5] Brenden Hills, The Daily Telegraph, "'Insecure' Commonwealth Bank online site led to $1.1m fraud, victim claims,".



Because fraud methods are evolving, the system must allow users to quickly configure new scenarios, and indeed modify existing behavioral patterns. However, the impact of these modifications on fraud levels, the false positives they will generate and their impact on a bank's operational team, must always be understood. To gain this knowledge, systems must allow users to effectively simulate their changes across large volumes of historical data and deploy these into production environments in real time.

This capability can prove tremendously powerful. For example, the bank may be concerned about emerging vulnerabilities around certain IP addresses. Traditionally, this would have led to extensive, in-depth research by investigative teams over a protracted period, before drafting a business requirements document for the IT department, which would then put a scenario in place. However, this new capability revolutionizes the entire process. Not only does it allow banks to aggregate information as they go, it also enables them to evaluate in real time how many customers are using a particular IP address, in how many countries those IP addresses have been accessed, and how many known frauds they have been associated with. The results can be almost instantaneous, and the investigators can then decide if they want to deploy the process in a live production environment. What might previously have taken months can now be completed in a matter of minutes.

Further detection techniques can be added at this stage. These might include anomaly detection to determine new potential areas of fraud by examining current behaviors and predictive analytics, where historical information is used to identify suspicious behavior that mimics previous patterns. Social network analytics can also be deployed in this context to establish links between money mules and groups of fraudsters.

By using this hybrid of analytics methods, fraud cases can be detected early and accurately. In fact, time is of the essence throughout this whole detection process, and the system must be able to identify high-risk transactions in real time, potentially block them, and then route them to the relevant investigators for review.

Hybrid analytics enables financial institutions to not only understand today's challenges and implement technology to address them, but also deliver the necessary flexibility to enable them to evolve and adapt to counteract the ever-changing approaches and behaviors of the threat.

But the process cannot rely on technology alone, and users must be empowered to spot new trends and emerging operating methods. This means putting data in the hands of the users, enabling them to quickly and easily drill down to explore areas of risk not previously considered. This gives them the power to ask questions on the fly, without the need to rely on IT, and with the results presented in a user-friendly and highly visual way. The knowledge gained here can then be fed back into ongoing detection models, enabling the system to stay ahead of the curve.

One Step Ahead

The fraudsters are currently setting the pace in the long-term battle with the banks, and the rate of online fraud is increasing, with inventive criminal gangs continuing to develop new fraud techniques in order to endlessly probe the banks' defenses.

In this complex, fast-moving environment, financial institutions will increasingly benefit from a hybrid analytics approach to fraud detection that enables them to not only understand today's challenges and implement technology to address them, but also deliver the necessary flexibility to enable them to constantly evolve and adapt to counteract the ever-changing approaches and behaviors of the threat.

For more information please visit: sas.com/fraudfinancialcrime