

Addressing Fraud in Real Time Payments



Pressure from customers and regulators is forcing banks to improve the speed at which an interbank payment reaches the beneficiary's account. While many countries are moving to a one-day process, some are moving to a real time process. The United Kingdom is one of those countries moving to a real time process with an initiative called U.K. Faster Payments.

The U.K. Faster Payments initiative effectively makes electronic payment funds — either account transfers or bill payments — available instantly, thereby eliminating the current three- to four-day waiting period.

From a customer perspective, the ability to send and access funds in real time provides significant benefits in terms of convenience and financial management. Unfortunately, the rapid availability of funds makes the U.K. online banking system an attractive target for criminals — especially since other initiatives, such as chip and PIN, have limited the ability to make fraudulent card transactions.

This document explores the challenges of fraud in the real time payments world and the techniques available to address the challenge.

The Threat of Fraud in a Faster Payments Environment

Online banking fraud can be perpetrated in a number of ways; however, the general modus operandi remains similar: compromise the account login and password through phishing, Trojan horses, SQL injections, etc.; log into the account via an institution's online portal; and transfer money into another account that the fraudsters can readily access.

Although Faster Payments is a new initiative in the United Kingdom, other countries such as Australia, Canada and Turkey have been operating under a similar system for some time. In order to profit from the availability of funds in this system, each country has had to implement its own defenses against the threat of organized crime.

The combative methods and techniques applied by financial institutions successful in mitigating online banking fraud follow the same basic principles. Although no empirical data exists for Internet banking fraud in these countries, anecdotally Australia suffered an increase in losses of more than 600 percent in 2005, and Canada and Turkey experienced similar loss increases.

Industry publicity regularly exhorts bank customers to be alert to phishing, discouraging them from divulging their Internet banking security information. Nevertheless, a recent survey showed that 70 percent of Australian banking customers did not know what phishing is. This suggests that phishing attacks will continue to lead to compromised accounts for some time to come. In fact, in a recent Galaxy survey of 647 Internet users commissioned by eBay, one in three Australian Internet users responded that they believe people must be “dumb” to fall for a phishing scam, yet 72 percent of respondents were engaging in risky online behavior.

Furthermore, the survey found that seven out of 10 Internet users are at risk of becoming phishing victims. Although 30 percent of Internet users responded that they know what phishing is, only 7 percent correctly understood what the term meant.

Fraud in Real Time Payments

Preventing Fraud in a Faster Payments Environment

One approach to prevent online banking fraud is the use of two-factor or multifactor authentication methods. These can range from tokens on key fobs to one-time passwords delivered via Single Message Service (SMS). The downside to this approach is that the cost and customer inconvenience involved often make this approach prohibitive: supplying an entire customer base with tokens that can break or be lost often becomes an expensive exercise.

Over time, financial institutions have become increasingly savvy in their application of two-factor and multifactor authentication. Initially, in an effort to reduce costs, institutions sent limited one-time SMS passwords when a customer logged in, as well as for each transaction performed. Institutions revised this practice and now send these passwords only when a customer makes a suspicious or series of suspicious transactions. Now the need for multifactor authentication also sends a clear message to the consumer that this is a risky channel, thus some customers may turn away due to perceived risk.

However, market unresponsiveness toward two-factor authentication meant that financial institutions had to create an alternative that was both cost-effective and could be achieved without customer interaction. The solution was an event-based analysis that provides a digital footprint for every customer.

Nonfinancial indicators — such as IP addresses, session IDs, password changes, path tracking, etc. — have become the dominant indicators of fraudulent activity. Traditionally, neural network technology has been at the forefront of fraud detection methodology. Nonetheless, the dynamic nature of Internet banking-related fraud has prevented the models from keeping pace with tracking these vital components and they have subsequently become antiquated in this space.

As the traditional modeling approach is failing, the main approach banks have taken is to profile customer activity. All customer interactions can be categorized into event classes that incorporate both monetary and non-monetary actions. These are as follows:

- ▶ *Payment events* — Financial transactions such as funds transfers and bill payments
- ▶ *Login events* — IP address and session ID profiling
- ▶ *Password events* — Changes in logon passwords
- ▶ *Profile events* — Changes to customer demographic information (e.g., addresses)
- ▶ *Payee events* — Changes to external payee account details
- ▶ *Navigation events* — Changes to how a customer navigates an online Internet portal

In isolation, one of these events may not indicate fraudulent activity. When combined, however, they elucidate strong patterns of criminal intent.

Combating Fraud in a Faster Payments Environment

A key piece of fraud intelligence strongly indicates that genuine customers tend to make transfers and bill payments to the same regular accounts and billers. Alternatively, fraudsters will transfer money to an account or biller that the genuine customer has never used. Account profiling is a technique that enables institutions to cross-reference all external accounts with which a customer has transacted in the last 12 months against each new transfer. When a transfer occurs to an account the customer has never used before, the institution can analyze that transaction in greater detail.

Another powerful indicator of online banking fraud is analyzing the login event — particularly IP address profiling. A static IP address provides each computer a unique identifier on the Internet. Once a series of online accounts has been compromised, fraudsters often log in from a single location to illegally transfer funds. The criminal's IP address can be captured and maintained in a blacklist, and any future login attempts from blacklisted IPs will automatically decline access to the fraudster, effectively preventing fraud.

Dynamic IP addresses and IP substitution add an element to this process. Dynamic IPs allow Internet service providers (ISPs) to assign an available IP to a user who has connected at any given time. When disconnected, this IP can be reassigned to another

Fraud in Real Time Payments

user. These IP addresses can be referenced back to the ISP in a specific location. Fraudulent IPs rarely come from the same ISP in the same location.

Customers tend to log in from the same IP ranges, such as work, home, school and sometimes public access points like a local library. IP profiling has been successful in capturing these regular IP ranges for individual customers and comparing them against the IP at login. Used in conjunction with a payment event — such as a large-value transfer — or password event — such as a recent password change — IP profiling has been a successful indicator of fraudulent activity.

An example of payee event monitoring is a specific attack that was occurring in Australia during 2006. Most Internet banking portals allow customers to store details of their regular billers. In the Australian case, once an account had been compromised, fraudsters were replacing the destination account number of these payees with a fraudulent account. In addition, they were future-dating transfers to these particular payees. Customers were unaware that the payee account details were changed, and to the financial institutions it looked as though the customers were making their regular payments.

An enterprise environment where all channels and information are monitored simultaneously has provided substantial benefits in preventing online banking fraud and identity theft. An institution in Australia has initiated call center validation into its enterprise risk management (ERM) capabilities. If a caller cannot pass the

customer validation questions (e.g., mother's maiden name, first pet's name), then the failure event is passed to the institution's ERM system. Analysts then use the information to make decisions. Furthermore, other short-term events — such as a large transfer, password or address change, or out-of-profile IP — are flagged as suspicious.

Initiatives like U.K. Faster Payments offer many benefits to both customers and the financial industry, as well as provide a more fluid and advanced payment system. Nevertheless, the threat of online fraud is extreme. Institutions that are inadequately prepared face the prospect of enormous fraud losses and substantial damage to their reputations. Proven solutions like those that have been implemented in other countries will significantly mitigate this risk. The benefits far outweigh the risks for institutions that adopt these measures.

About ACI Worldwide

ACI Proactive Risk Manager has been one of the market's leading fraud management solutions since 1998, with expertise in managing fraud from the point of compromise to resolution. ACI delivers regular releases of Proactive Risk Manager to ensure that our customers stay abreast emerging and evolving fraud trends. ACI Proactive Risk manager is used by 130 organizations every day to monitor, prevent and detect fraudulent transactions. Since 1975, ACI has provided software solutions to the world's innovators. We welcome the opportunity to do the same for you.