FIGHTING ONLINE FRAUD: AN INDUSTRY PERSPECTIVE

Volume 3
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Cybercrime and Online Fraud: An Evolving Threat</td>
<td>3</td>
</tr>
<tr>
<td>Fighting Online Fraud Requires a Multi-Layered Approach</td>
<td>5</td>
</tr>
<tr>
<td>Conclusion</td>
<td>7</td>
</tr>
</tbody>
</table>
In an ideal world, there would be no need to worry about online fraud. Unfortunately, we don’t live in an ideal world. The threat of online fraud is significant and here to stay. While this might be ideal for the fraudsters, it’s certainly not for the banks.

Regardless of a financial institution’s size or operating footprint, if they provide customers with online banking access, they face the threat of fraud via that channel. Cybercriminals and hackers routinely seek out and uncover weaknesses in a bank’s fraud defenses. Without a continuous improvement mindset that tests and retests the bank’s fraud defenses, cybercriminals will often exploit gaps quickly, quietly and be long gone before the bank or its customers uncover a problem. Although in some cases the attacks are not as silent or under the radar, but more on that later.

Given the inherent complexity of the online banking platform (and the dramatic increase in mobile banking), preventing online fraud presents financial institutions with a number of highly complex challenges to overcome. Preventing online fraud requires a layered and risk-based approach that does not place excessive reliance on a single tool or tactic to stop all threats. In fact, national and regional agencies like the Federal Financial Institutions Examination Council (FFIEC) in the U.S. and Committee of European Banking Supervisors (CEBS) in Europe provide guidance on these types of layered and risk-based approaches.

Since online banking provides an extremely cost-effective service delivery channel, by putting too many security measures in place to prevent fraud, financial institutions run the risk of impacting and inconveniencing customers. Similarly, customers need to be made aware of what is expected of them and the role they play in prevention.

This paper details the types of online fraud threats that financial institutions face, the various solutions that they have at their disposal to detect and prevent fraudulent activity, and the challenges banks face in educating their customers on how to avoid becoming a victim.

1 CYBERCRIME AND ONLINE FRAUD: AN EVOLVING THREAT

There is a virtual arms race taking place online between financial institutions and cybercriminals. As soon as a bank deploys a new process or technology to prevent online fraud, cybercriminals find a weakness to exploit. As banks amend and adapt their approach to fraud prevention, so too do cybercriminals. In fact, banks often end up several steps behind criminals due to the fact that they are more constrained by regulation, budget and personnel resources, and “red tape”, among other inhibitors. These pose considerable
headwinds for banks compared to the bad guys, who are not limited by similar constraints.

With every new banking service, such as mobile banking, a new set of fraud risks emerge. The theft of credentials to perform illicit activity, known as account takeover (ATO), may include identity theft, ACH and wire fraud. These are just some of the types of online fraud that financial institutions must guard against. ATO, where the cybercriminal assumes complete control of an account, is a big threat in the online channel and can be particularly problematic. Since the customer loses control of their account — albeit for a brief period — it is a more invasive form of fraud that impacts the customer’s sense of personal safety and security. Consequently, banks may find it more difficult to retain a customer impacted by ATO activity.

To perpetrate online fraud, cybercriminals employ a range of tactics that target people, processes or technology separately or in combination. The following includes some of the more commonly used tactics:

Malware: Criminals have a number of tools at their disposal to infect a customer’s computer with malicious software or malware. The knowledge it once took to hack a site has fallen considerably. In fact, tools which are easy to procure (e.g., Blackhole exploit kit) and are inexpensive have brought more access to the less sophisticated hacker.

Most often, the fraudster sends an email that convinces the recipient to click on a link (known as phishing), which in turn downloads the malware directly to the users machine or routes the user to an infected but legitimate website where they will face the same threat from a seemingly harmless source. Once installed, the malware captures the customer’s keystrokes, including their bank login credentials, and sends the data to the criminal. Within minutes of receiving the customer’s credentials, the cybercriminal accesses the user’s bank account and initiates fraudulent transactions. Otherwise, the fraudster will wait for the customer to access the bank and steal their session directly in real time, unbeknown to the customer — this is known as man in the browser (MITB).

Social engineering/vishing whaleing: Although not as high tech as the use of malware, gathering data via social engineering can often help criminals overcome a bank’s fraud defenses. Social engineering can involve the customer and/or the bank. For example, a criminal may call the customer at their home or office and pretend to be an employee of the bank’s fraud department that wishes to verify a pending transaction (this practice is known as voice phishing or vishing). During the call, the anxious customer willingly provides information regarding their account that the criminal uses to commit fraud. Alternatively, the criminal may call a bank’s call center with incomplete data regarding the customer’s bank account or identity. During the call, the criminal subtly extracts information from the bank employee that they then use to access online banking and commit fraud. Other forms of ATO include whaling, targeting the “big fish” or upper management in a more direct email. The objective here is to get access to confidential or critical data which might reside on an executive’s hard drive.

Exploiting a weaker online platform: Let’s face it, managing user names and passwords for a multitude of banking, gaming and social media sites can be overwhelming. Unfortunately, it is human nature to use the same login credentials at more than one website. Also, the number of passwords required today makes it difficult for end users to remember from site to site (believe it or not, “password” is still one of the most common passwords used today). Consequently, by compromising one site, criminals may gain access to credentials to many others by exploiting the re-use of a password. As an example, a breach that takes place at an online retailer which exposes the customer’s login credentials may also result in fraud within the banking sector.

Short Message Service phishing/smishing: With the explosion in smartphone usage, criminals have found a new way to gather the data they need to commit fraud. Similar to a phishing email scheme, smishing sends a text message, sometimes even described as a “fraud alert” that asks the recipient to provide personal information such as their online banking password, or make a phone call to a number controlled by criminals, and enter their ATM PIN number or online password.

Denial of service/distributed denial of service: A denial of service (DoS) or distributed denial of service (DDoS) both have the same aim — to block a site from use by legitimate customers. The difference is that a DDoS attack involves many machines attacking or tying up a financial institution’s servers with time consuming tasks, whereas a DoS involves just one machine attempting to overload the firm’s website. DDoS attacks are far more complex and difficult to defend against since they involve a number of attackers. The DDoS attacks are often created as a diversionary tactic. While critical risk and security teams are focused on restoring service, other sinister activities can take place elsewhere in the name.
of stealing information, money or both. While the connection to actual fraud loss and DoS/DDoS is rarely publicized, a case involving a loss of $900,000 indicates that it does happen.¹

**Involvement of a bank's insiders:** Most bank employees have access to customer data; therefore, cybercriminals often attempt to coerce, bribe, blackmail or trick them into disclosing such information. Fraudsters may also target employees in the bank’s fraud department tasked with reviewing suspicious transactions with the goal being to ensure that their transactions pass scrutiny. Without the proper tools and compensating controls in place, detecting questionable insider activity can be particularly challenging since bank employees typically need access to customer data in order to perform their job.

Cybercriminals may employ the tactics noted above independently or in combination. If an approach is effective, fraudsters will continue to use it.

In order to commit fraud, cybercriminals readily adopt new forms of technology. In fact, numerous articles and reports note that cybercriminals constantly innovate. The following quote from an article written by Victoria Baines, the head of the Strategy and Prevention Team at the European Cybercrime Centre, notes the following:

“Cybercriminal businesses are constantly innovating. As well as making extensive use of social media to distribute scams and links to malicious software, they scan the environment to identify new software vulnerabilities, new environments popular with internet users and new attack vectors.”²

Today, cybercriminals carry out activities almost with the same innovative spirit as a growing business. Cybercriminal call centers, black market eCommerce sites and fraud-as-a-service (FaaS) entities corrupt traditional business models with the sole aim of defrauding the public and private sectors alike. Since cybercriminals embrace innovation, so too must financial institutions. Assuming that today's fraud defenses will always prove effective in preventing online fraud is a fatally flawed assumption.

Many of the approaches that cybercriminals employ take advantage of the customer’s lack of knowledge, and specifically, their failure to appreciate the risks associated with accessing the internet and responding to unsolicited emails. Helping customers understand the importance of protecting their login credentials, using different passwords over multiple sites or using complex passwords, for example, should serve as a cornerstone of every bank’s fight against fraud. With the emergence of each new payment type, banks must revisit the fundamentals of fraud prevention with their entire customer base.

To avoid being ignored, banks must use different approaches to educate their customers such as placing notices on their website, using inserts to accompany bank statements and utilizing posters positioned in high traffic areas within branches. By getting customers involved in the fight against fraud and making them aware of what is expected of the customer and what is not when it comes to sharing data and communicating/interacting with them, banks put some of the power back in customers’ hands to prevent losses. It also helps send a clear message that fighting fraud requires a partnership between the bank and its customers. Notwithstanding the difficulty associated with measuring the effectiveness of an education campaign, financial institutions must continue to amend and revise their approach as the threat landscape changes.
hostile online environment. Recommended protocols like these help give financial institutions guidelines for a multi-layered approach.

Although there isn’t a “one-size-fits-all” portfolio of fraud tools and tactics that is applicable to all financial institutions, approaches do exist that can prove highly effective in preventing online fraud:

- **Multi-factor authentication**: Involves the comparison of data gathered from the customer, such as user signature, name, password and something only the user knows, against information provided during the account opening phase or at some point during the life of the account. Additional factors may include tokens that generate random numbers the customer inputs, a USB device containing login credentials, or information about the customer’s device that the bank captures and associates with the account “behind the scenes.”

- **Geolocation**: Based on the IP address associated with the customer’s location, or what appears to be their location, a bank can block or subject a login to additional scrutiny, such as out-of-band authentication. Since a great deal of online crime emanates from overseas, identifying the location of the device that is connecting to the bank’s website can help identify higher risk transactions. Some criminal organizations know that banks use geolocation; therefore, they take steps to mask their true location by altering the IP address. Knowing that a device is located overseas is not sufficient to justify blocking a login or transaction since doing so may prevent a legitimate customer who is traveling or based overseas from accessing their account. In order to leverage the intelligence gathered by a geolocation tool, banks often layer or incorporate the data as part of a larger fraud detection platform to derive an adjusted risk factor that includes additional variables such as the type of transaction or intended payee, etc.

- **Device recognition**: Since online banking involves a device such as a laptop, mobile phone or tablet, identifying each device can help prevent fraud. Device recognition analyzes and assigns a unique identification code to each machine that visits an online banking platform. Device recognition software typically includes a database of devices previously connected to fraudulent online activity. If the software identifies a device connected to previous instances of fraud attempting to access online banking, the bank can choose to block access.

- **Transaction monitoring**: Software reviews a customer’s activity for anomalies or red flags, which are indicative of fraud. Transaction monitoring software captures data regarding the transactions. This could include monetary or non-monetary data, including the date and time requested, the payee account and name, the account number and the method used to initiate the ACH. If the bank suspects fraud, they may contact the customer directly to confirm the request.

- **Navigation controls**: Focusing on software or rules that monitor and analyze navigation of the web session against the expected behavior. This protocol may include analyzing web logs, site visits, viewing trends and other variables.

- **Cross channel**: Monitors and analyzes user behavior across a range of payments and channels to determine if there is a correlation between behavior and the probability of fraud.

- **Entity link analysis**: Discovering the relationships between devices/users/accounts to help identify the potential that there are links between the entities and their attributes.

Creating profiles based on customer behavior over periods of time is also likely to be employed as part of a transaction monitoring solution. Profiling generally includes the usage of historical trends, previously identified fraud scenarios within a peer group and usual transaction amounts, etc. to minimize the frequency of false positives or unintended alerts regarding legitimate good customer behavior. Enhanced profiling activities can track statistics over a chosen time cycle for a financial or non-financial data element(s). These types of monitoring activities elevate the predictive nature of finding fraudulent activity.

For banks to be competitive with the current threats of cybercrime, they must create risk-based layered fraud defenses rather than simply relying on one layer or approach. Financial institutions must embrace a portfolio of security-related tools, strategies and tactics so that they continually test, retest and revise their strategy based on the changes in the threat landscape.
Customers love online banking for its convenience, while banks benefit from lower costs and a greater reach than a physical branch network provides. To ensure that both parties continue to benefit from online banking, it must remain a safe and secure channel that allows legitimate customers access as needed, while simultaneously blocking entrance to cybercriminals.

Cybercriminals will continue to target online banking for as long as it is worth their effort to do so. Each instance of online fraud helps fuel additional investment by cybercriminals in the people and technology they need to overcome a bank’s defenses.

Educating the customer on how to help prevent online banking fraud is just one element of a bank’s fraud defenses. Deploying advanced technology that can quickly adapt to the changes in the cybercriminal’s modus operandi is essential to protecting the online channel. Customers must have confidence in the security of a bank’s online platform. There is no end in sight, but banks must stay committed to winning each battle they fight to prevent online fraud.

---

   http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/

ACI Worldwide, the Universal Payments (UP) company, powers electronic payments for more than 5,100 organizations around the world. More than 1,000 of the largest financial institutions and intermediaries, as well as thousands of global merchants, rely on ACI to execute $14 trillion each day in payments and securities. In addition, myriad organizations utilize our electronic bill presentment and payment services. Through our comprehensive suite of software solutions delivered on customers’ premises or through ACI’s private cloud, we provide real-time, immediate payments capabilities and enable the industry’s most complete omni-channel payments experience.

LEARN MORE

WWW.ACIWORLDWIDE.COM
@ACI_WORLDWIDE
CONTACT@ACIWORLDWIDE.COM

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

© Copyright ACI Worldwide, Inc. 2017
ACI, ACI Worldwide, ACI Payment Systems, the ACI logo, ACI Universal Payments, UP, the UP logo, ReD, PAY.ON and all ACI product names are trademarks or registered trademarks of ACI Worldwide, Inc., or one of its subsidiaries, in the United States, other countries or both. Other parties’ trademarks referenced are the property of their respective owners.

ATL6318 05-17