High-tech robbery: The new intersection of cyber crime and financial fraud

JANUARY 20, 2016

by Maribeth Mallon Haynes
Portfolio Manager, Counter Fraud and Financial Crimes, IBM
Follow me on LinkedIn

The 1930s in America marked an era of violent bank robberies and deadly shootouts with legendary characters such as John Dillinger, Pretty Boy Floyd and Baby Face Nelson. However, the most successful bank robber from the Great Depression era often didn't use a loaded gun. Instead, Willie Sutton used clever disguises and slick talking to steal more than $2 million.

If Sutton were alive today, he'd be a hacker. Modern bank robbers use software tools and programming expertise to accomplish the same outcome as their 20th-century counterparts. And, unlike the lone wolves of the 1930s, cybercrime has become big business: court documents in a recent online fraud case refer to the defendants as members of a "diversified criminal conglomerate." No wonder banks are investing heavily in fraud detection, prevention and remediation measures.

Exploiting gaps

And yet the problem—and the financial costs—continues to grow. Consider one key area: fraud incidents involving wire transfers have nearly doubled in the last two years. Cyber robbers have become adept at perpetrating fraud using a series of seemingly unrelated actions that combine cybercrime and fraud. Such complex attacks fly under the radar of prevention tools, which tend to be focused either on cybersecurity or fraud, but not both.

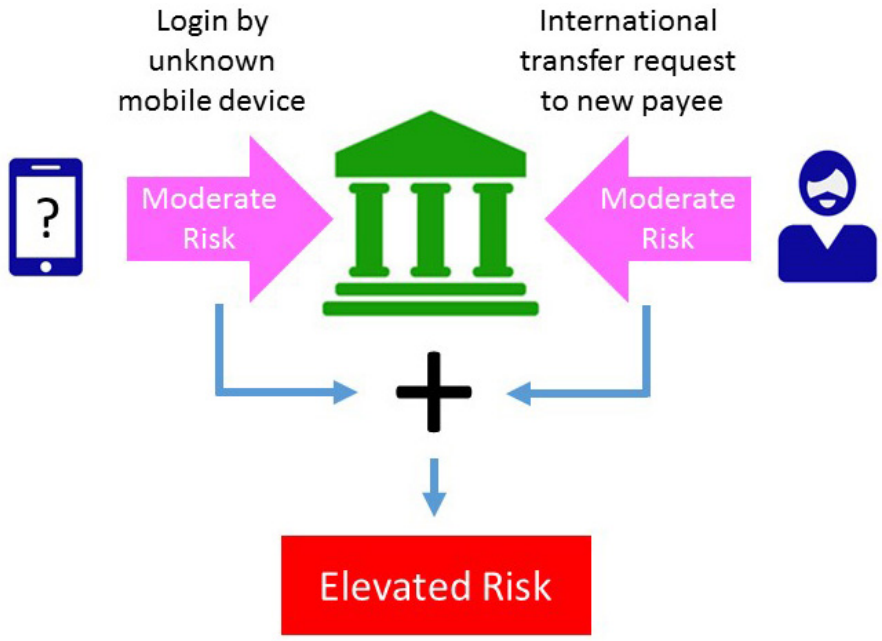
Many fraudulent wire transfers start with the theft of login credentials for a legitimate bank customer—unfortunately, a relatively common cybercrime today. The would-be fraudster then uses the stolen username and password for a sequence of routine activities: open a new account, add a new international payee, transfer funds between accounts and request a fraudulent wire transfer to the new payee—the cybercriminal. None of these actions individually look suspicious to antifraud investigators, but if they all are accomplished, the bank's losses can be substantial.

Fighting back with technology

Never was the adage "fight fire with fire" more appropriate than in the case of counter fraud strategy. Just as the fraud perpetrators are becoming more sophisticated, so must banks' defenses. The key technological innovation needs is to correlate the information from individual cybersecurity and fraud prevention tools. When cybersecurity and antifraud countermeasures work together, they can prevent many of the exploits that currently slip through today's siloed defenses.

Consider how correlation would work in the wire transfer example. Security software such as IBM Trusteer detects a login from an unknown mobile device. Using a low-moderate-elevated-high risk rating system, this incident is rated as presenting moderate risk—that is, something to keep an eye on but not overly alarming by itself.

A short time later, a bank customer initiates an international wire transfer to a new beneficiary. In the absence of any other alerts, a counter-fraud tool such as IBM Counter Fraud Management assesses this transaction as moderate risk—again, no smoking gun. However, when the two events are correlated, clearly a coordinated exploit is underway. Notified of the existence of an elevated risk—a more accurate assessment of the situation—a fraud investigator blocks the requested wire transfer and stops this fraud attempt dead in its tracks.



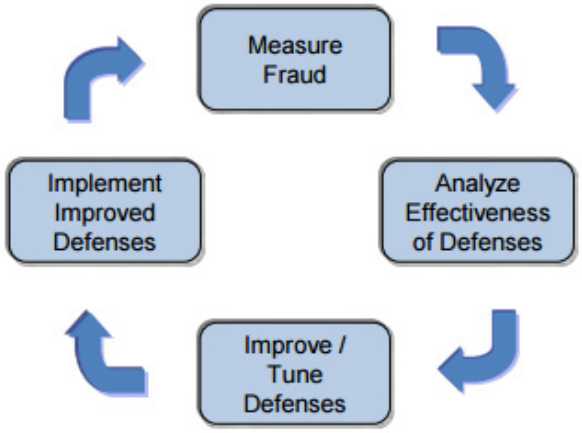
Best Practices for Reducing Fraud

Beyond upgrading their counter fraud technology, there are additional steps that banks can take to help reduce their fraud losses. From the organizational perspective, foiling fraud attempts must be top priority for everyone in the bank. The departments responsible for fraud—anti-money laundering, cybersecurity, operations, even human resources—need to work together to ensure that anomalous activities detected anywhere in the organization are communicated to all stakeholders. Executive sponsorship is particularly important: As one executive puts it, counter fraud must move from the security room to the boardroom.

Leading institutions are taking control of their fraud risk by applying counter fraud best practices such as:

- Measure continually. Keep detailed records of actual and attempted fraud.

- Analyze effectiveness of defenses. Use records to determine how much is being caught by your current defenses and identify areas for improvement.
- Tune defenses. Continually reallocate resources and fine-tune rules.
- Never stop improving your antifraud posture. Treat measuring, analyzing, and tuning as on-going activities to be supported with permanent human resources and fully supported, integrated tools.



Collaboration and correlation are becoming important—perhaps even essential—approaches for defeating ever more innovative fraud schemes. If you are involved in structuring your bank's antifraud defenses, learn more about the intersection of cybercrime and fraud, and what you can do about it.