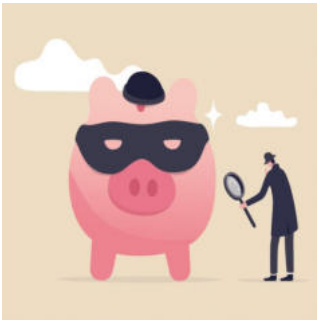
Cybersecurity Digest

Bi-Weekly Update by the O/o CISO of Meghalaya Rural Bank

Volume 2 Issue 18 **Date: 16.12.2025**

Bank Drop



A bank drop refers to a bank account controlled by a criminal, used as a pivot in financial system conceived to launder illicit gains. It is either created through fake credentials or stolen to an unsuspecting victim. In some cases, money mules can also be used.

A bank drop is essential in money laundering schemes, as it is often used to legitimize and conceal the proceeds of illegal activities. It can support cybercriminals engaged in layering and structuring activities, as part of their money laundering process. Financial systems are now strongly monitored against money laundering activities. Therefore, elaborated financial structures are developed to wash out the proceedings of their activities.

In the very beginning, bank drops involved physical manipulation, such as forgery. With the rise of Internet, cybercriminals shifted gear and were able to carry their operations remotely. Although there are plenty of methods to obtain one, more advanced techniques such as breaching into banks' information systems or spear phishing made their appearance. Automation bank drops' networks also allowed organized crime to streamline their financial operations.

As cybercriminals continue to exploit the digital landscape, the connection between bank drops and cybercrime is very intricated. Because digitization and automation made a huge impact on financial systems, cybercrime also took the opportunity to become more sophisticated electronically. Moreover, cyber-enabled crime now represents an increasing part of the puzzle. Ransomware is now a looming threat over companies, and individuals face waves after waves of phishing attacks and account takeovers.

Alongside bank drops, cybercriminals have also evolved in their money laundering techniques. They now operate complex schemes involving shell companies, countless accounts and international transfers to obfuscate the origin of their illicit funds.

How do bank drops work

Bank drops usually follow a series of coordinated steps:

- **Credential collection:** At first, the cybercriminal will usually gather identity information to create a bank drop, either by stealing or purchasing someone's credentials or even creating a synthetic identity. To make it legitimate, it may also create a comprehensive ecosystem with an email address, burner phone, and IP address to replicate the victim's environment;
- **Selecting a bank:** Once the identity is well-crafted, the cybercriminal will find an appropriate bank to open an account. It may leverage a money mule to do it on his behalf and further protect itself from detection. The bank selected would have preferably weaker controls over identity information;
- **Legitimizing the account:** After the account is opened, few legitimate transactions will be conducted to give it a clean state, and avoid raising any red flags;
- **Operating the bank drop:** If all goes well, the bank drop will then be used to receive the money from illicit activities. This will be combined with money laundering techniques to distance the funds from their illegal origins;
- **Withdrawing the funds:** Finally, after the funds have been laundered or moved to different accounts, the perpetrators proceed to withdraw the money as cash, transfer it to offshore accounts, or utilize it for personal gain. This step aims to obscure the trail and make it challenging for authorities to link the funds back to the initial illegal activities.

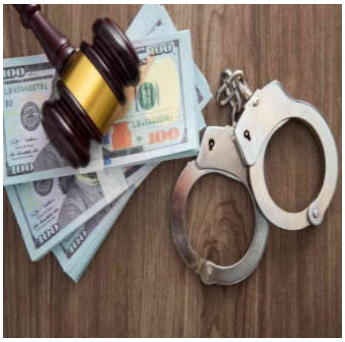
Why bank drops are so nefarious?

Even though bank drop aids and abets the money laundering of criminal activities, it is also the result of other crimes such as impersonation, identity theft, or penetration of information systems. Since bank drops often serve as a gateway to other criminal activities, funds laundered through them may be used to finance and facilitate additional illegal operations, such as drug trafficking or terrorism.

Given the bank drop's key role in money laundering schemes, it can cause tremendous damage and deeply undermine the trust in financial institutions. On the other hand, banks that fail to prevent those activities may face important fines from regulators, but also administrative sanctions.

Victims of identity theft can also suffer the consequences of bank drops and put them at risk as their identity can be used to conduct additional illegal activities. As it also relies on the recruitment of money mules, lured by promises of easy money, bank drops can put them at risk of becoming accomplices to criminal activities.

What measures can be taken to tackle bank drops



Given the severe consequences of bank drops, comprehensive for the civil society as a whole, measures to tackle it are necessary. While everybody can play a role from law enforcement to individuals, financial institutions are the key players in combatting bank drops. As technological advancements are now allowing cybercriminals to automate the creation of bank drops, financial institutions need to implement different measures to mitigate this risk:

- **Raise awareness among employees and customers**: Employees are sometimes the first line of defense. Training employees to detect such threats, but also raising awareness among customers can prove to be powerful to detect and limit bank drops;
- **Ask for customer information:** Thorough checks make for full-proof financial environments. When in doubt, operators should always ask for more information, to determine origin of funds or customer's identity;
- **Establish risk-based transaction monitoring systems:** Detecting suspicious transactions is essential to identify bank drops. Between behavioral analysis using algorithms to analyze patterns, deviations alerts and risk scores, robust transaction monitoring system can prove as a useful ally against bank drops;
- **Implement comprehensive anti-money laundering (AML) programs:** By developing adequate deterrence policies based on customer account usage, enforcing strong due diligence processes to obtain relevant information on the customer, a comprehensive AML program not only allow financial institutions to comply with current regulations, but also empowers them against multiple threats;
- **Cyber security measures:** Enforcing robust two-factor authentication (2FA), but also implementing advanced threat detection can boost how financial institutions deter bank drops.

Prevention of Cybercrime

- Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
- To prevent cyber stalking avoid disclosing any information pertaining to one self. This is as good as disclosing your identity to strangers in public places.
- Never send your credit card number to any site that is not secured, to guard against frauds.