
# The Battle Between Corporate Treasury and Fraudsters is Getting Personal

## Biometric Tools Can Help Corporates Improve Cyber Security

**Rajesh Shenoy**
Global Head,
Digital Security,
Treasury and Trade
Solutions, Citi

Businesses today face a formidable foe in the form of cyber criminals. A recent report estimates that monetary losses globally from cyber crime is expected to reach a staggering $6 trillion annually by 2021.[1] According to the Association for Financial Professionals (AFP) 2018 Payments Fraud Survey, a record 78 percent of treasury organizations were victims of payments fraud in 2017 alone.

Going toe-to-toe with the cyber criminals is a tall order given that the playing field is not level. They can change and adapt very quickly and are not beholden to rules, regulations or legal boundaries. Their operations are often low profile, low cost and low risk. If one approach doesn't work, cyber criminals can simply shift to another until they have succeeded. And what's worse, they are collaborating with each other on the darknet by sharing tips, tricks and software code.

[1] *Source: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/*

Corporate treasury departments, on the other hand, typically have strict protocols to follow and limited resources available to defend valuable assets. Being smarter and more aggressive in cyber security is an imperative as the threats become increasingly perilous. Beyond the very real financial costs, corporates must also consider the risk of business disruption, loss of data and data privacy, along with the threat of reputational damage should a cyber security incident become public.

Fortunately, emerging technologies are being explored that offer important opportunities to fight back and help defend against these malicious cyber threats.

## Better locks on the door won't be enough

With any kind of security improvement come trade-offs. In the physical world, that means more locks to unlock and more alarm codes to remember. In the digital world, it means continuously changing strong passwords and using two-factor authentication. In short, more security can mean more inconvenience and less accessibility.

New advances in digital security are changing this equation. Factoring in the login patterns of authorized users of digital finance channels between corporates and banks has become an important tool in the cyber security arsenal. For example, statistical data, such as the date and time when clients normally log into the bank's platform, can be used to help detect unusual behavior. Logging in at different hours could be a sign of an unauthorized transaction, which would automatically trigger additional security procedures to confirm the identity and authority of the user.

Whenever a new device attempts to access sensitive information, additional controls necessitate that the user verify that they have adequate permission. At the same time, notification is sent to the authorized user to alert them to the fact that a new device in their name is attempting to access their account. The physical location of the user is also factored into the authentication process. When IP address data is combined with date and time information, security protocols can detect when a user is trying to execute a transaction or access accounts from two widely dispersed geographic locations in a very short period of time — an indicator of very unusual, and potentially fraudulent, activity.

## Adding biometrics solutions to help enhance security

Those protections are now being enhanced with new methodologies. By adding active biometric authentication measures, such as fingerprint or facial scan technology to current password authentication protocols, security can be dramatically improved. These types of measures have the added benefit of being easy for the end user to implement and are not easily stolen or reproduced by cyber criminals.

An example of this can be found in Citi's recent introduction of biometric authentication in select markets, providing easy access to CitiDirect BE® desktop and mobile, the bank's core treasury platforms. Clients can now securely log in using fingerprint or facial recognition via the CitiDirect BE® App on their smartphones. Furthermore, this can be used to authorize access from their desktops. This process is known as out-of-ban (OOB) authentication. The user puts their login info on the desktop, validates their biometric information using the phone's technology, and is then authorized to access their account via the desktop. This replaces the multiple steps needed to copy codes from password generating tokens in order to log in, which is expected to greatly simplify and enhance the user experience.

The next wave of biometrics solutions being explored utilizes passive measures, also known as behavioral biometrics, to help further strengthen secure access and authentication processes, while making it more convenient for clients. These measures leverage data gathered from the interactions between clients and the bank to develop tailored risk analysis in real time, thereby helping to identify atypical (and potentially fraudulent) activity.

By looking at subtle behavioral patterns, such as typing cadence or site navigation trends, machine learning and big data analytics technology can be used to identify specific idiosyncrasies around how we work on our computers or mobile devices, creating the equivalent of a unique digital identifier. If the system detects that this unique pattern has suddenly altered, it suggests a new, possibly unauthorized user may be attempting to access the account or conduct a transaction. This would trigger an immediate response, requiring further verification so authentication could be confirmed. Best of all, in addition to bolstering security, these types of measures would typically take place in the background and be completely unobtrusive to the user (and invisible to hackers). While this technology is being explored and has potential added value today for use as a supplemental detection tool, it is maturing and evolving rapidly.

Such techniques will always be probabilistic and not authoritative or definitive, but they do have the potential to provide intelligent and insightful analysis aiding in the deployment of selective dynamic controls.

It's critical to highlight that in the case of Citi, which is exploring behavioral biometric in early testing stages, any biometric data will only be gathered and used for limited purposes, stored in highly protected ways, and never resold.

## The evolving nature of cyber security

As cyber threats constantly evolve, so too do the innovations to combat them. Citi, in particular, is continuously engaging with sophisticated technology and processes to help ensure clients are protected. The bank is activity exploring better methods of security in the biometric realm that are expected to provide greater measures of protection, while offering minimal inconvenience to the end user.

By adding layers of security to already proven methodologies, biometric tools hold tremendous promise for safer and more secure interactions between corporates and banks. As an industry that has a deep commitment to security, these advancements are an important evolution in the never-ending battle to protect vital client assets and information. ■

As cyber threats constantly evolve, so too do the innovations to combat them. Citi, in particular, is continuously engaging with sophisticated technology and processes to help ensure clients are protected.

Treasury and Trade Solutions
**citi.com/treasuryandtradesolutions**



1827842 03/19