BANK OF AMERICA

The Next Fraud Wave is Here

See how we're helping businesses fight back

Global cybercrime costs will grow by 15% per year over the next five years, reaching $10.5 trillion annually by 2025, up from $3 trillion in 2015.[1] While defenses like chip-and-PIN cards have made card counterfeiting nearly obsolete, today's greatest risk is now to digital systems. Connected devices, proliferating data and the shift to mobile offer new ways for fraudsters to commit cyber crimes, which is why we're helping clients identify evolving security gaps and devising new solutions to fight back.

Security gaps in a changing world

Ironically, the advances that make business more convenient can also make it easier for fraudsters. The Internet of Things (IoT) enables smarter cities, homes and hospitals, but the security of their connected devices is often not as smart. The sharing economy — decentralized platforms that allow users to share rides, apartments and more — is relatively untested and can lack user accountability. Connectivity and digitization, which are driving exponential growth in data and analytics, can raise major privacy concerns. Moreover, millennials are now entering the workforce in larger numbers, bringing with them an always-on digital lifestyle that tempts users to trade security for convenience.

These gaps can lead to vulnerabilities. For instance, a recent worldwide exam of smart-city systems found security flaws that allowed unauthorized access to traffic, weather-alert and other infrastructure.[2] Cybersecurity firm Check Point released new statistics that show a 45% increase in cyberattacks since November against the global healthcare sector, over double an increase of 22% against all worldwide industries in the same time period.[3] Even an internet-connected aquarium or thermostat — which may seem innocuous — could be a gateway for cyber criminals to penetrate sensitive business systems.

Prevalent fraud types

Three types of sophisticated threats are prevalent today.

- **Identity fraud** occurs when thieves use stolen Social Security or passport numbers to create a synthetic identity, which is then used for fraudulent transactions.
- **Digital account fraud** refers to taking over a real person's legitimate account to launch bot and malware attacks, and is often run by "human farms" in low-cost countries.
- **Payment fraud** includes credential theft, chargeback and other threat methods during payment authentication or dispute.

While each of these fraud types is unique, they can occur across the entire spectrum of a transaction from account access all the way to customer service.

Key takeaways

- Connected devices and proliferating data can create new ways for fraudsters to commit cyber crimes
- Identity fraud, digital account fraud and payment fraud are among today's most sophisticated threats
- BofA is helping clients identify security gaps and devising new solutions to fight back

Three pillars for fighting back

A strong defense requires **data sharing** across the entire organization, which promotes greater transparency and decision-making. **Securing all touch points**, including user credentials and digital platforms, can reduce unauthorized system and account access. **Eliminating cardholder "friction"** or pain points can also be extremely powerful. Friction can lead cardholders to non-secure behavior, such as writing down passwords that are hard to remember or using the same password in multiple places.

Biometric authentication can be a great way to layer these pillars and increase their impact, especially as more business shifts to mobile. Requiring fingerprint or iris scans can help secure devices and systems while eliminating friction. The next wave is "passive biometrics" or "device intelligence" in which the device "learns" how its owner typically holds and handles it, adding yet another layer of authentication. While not yet widespread, device intelligence shows great promise and is already being built into the future of eCommerce.

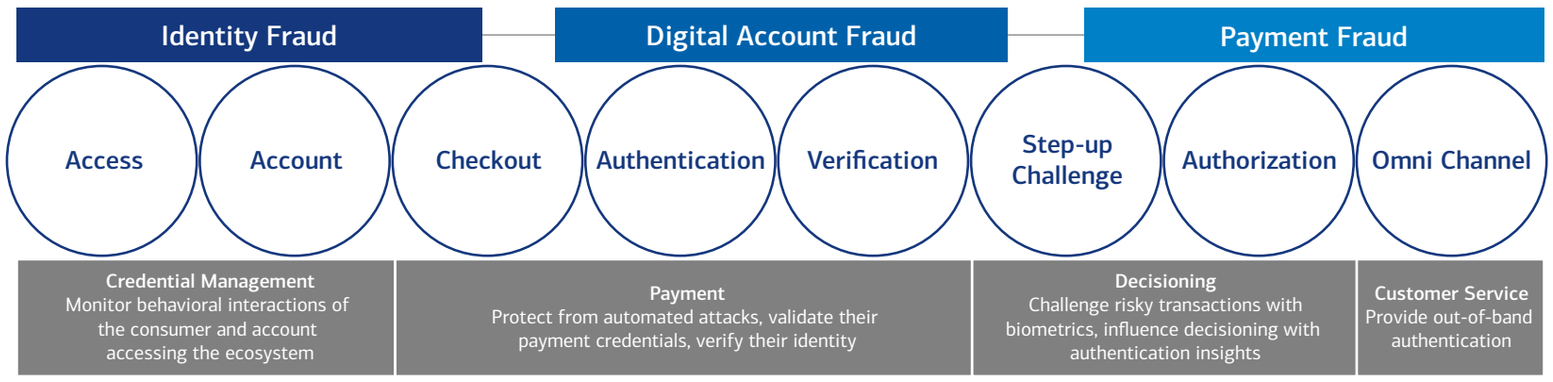
Additional safeguards

Other anti-fraud strategies are more straightforward, such as shifting more purchasing to virtual card, where every transaction gets a single-use account number — making fraud much less common. Splitting card-request and payment-approval duties among several program administrators is another effective safeguard.

Bank of America is also enhancing our commercial card program with extra security layers. We've begun requiring cardholders to enter one-time-passcodes — delivered via text or email at the point of sale — to authenticate certain transaction types. We've also stopped allowing "PIN bypass" at some types of merchants where card misuse trends higher. Our cardholder website is now mobile-friendly and more robust, enabling users to set up real-time transaction alerts and temporarily shut down their cards when there are no immediate plans to use them. All Bank of America commercial cards are now compatible with Apple Pay, Google Pay and Samsung Pay, so our cardholders can use tokenization and biometric authentication for extra security.

These enhancements have greatly curtailed card fraud among our clients.

A layered approach to security



Enhancing treasury intelligence

As businesses seek to transform treasury, finding ways to work that are fast, smart and secure becomes more important than ever. An innovative card and payables platform can help make it happen by protecting systems, employees, customers and reputations.
Although the next wave of fraud and cyber threats is here, we now offer more ways than ever to help clients fight back.

BANK OF AMERICA

[1]Cybercrime Magazine, *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*, November 13, 2020.

[2]CNet, *Smart Cities Around the World Were Exposed to Simple Hacks*, August 10, 2018.

[3]ZDNet, *As coronavirus cases surge, so do cyberattacks against the healthcare sector*, January 5, 2020.