VISIT OUR FRAUD HUB

Forecasting the future of fraud

Our fraud prevention experts are studying recent trends to understand what cyberattacks may look like down the line—and help businesses prepare now.

continued on next page >

VISIT OUR FRAUD HUB

Fraud is snowballing

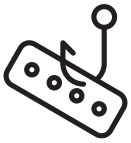
The total payment value of business email compromise (BEC) attacks is growing aggressively this year, up more than 100% in 2021 compared with the same period of 2020, according to Commercial Banking estimates.

Ransomware also poses a serious threat. Commercial Banking clients reported more than four times as many ransomware attacks in the first half of 2021 compared with the first half of 2020.

> *"Fraud is pervasive, and it's only going to keep growing. Bad actors are finding and exploiting weaknesses in companies' payment control environment, and every successful fraud improves the criminals' incentives for newer, bigger attacks."*
>
> John Geronimo, Executive Director and Fraud Strategy Director, Commercial Banking

THE FORECAST

Fraudsters, emboldened by the high value of a successful fraud scheme, will continue to escalate their attempts. With the disturbing rise of the ransomware-as-a-service business model, criminals can buy ransomware tools on the dark web as easily as your business leases software from legitimate developers. That means it's no longer necessary for criminals to have a sophisticated skill set to launch ransomware attacks. They don't need every attack to succeed to make off with a fortune—instead, they'll prey on as many targets as possible, as often as possible.



BEC is the main driver of fraud

Fraudsters continue to attempt BEC attacks—deceptive emails aimed at tricking victims into redirecting invoice payments to accounts that criminals control. The average amount stolen in a BEC attempt is up by 129% year over year, according to Commercial Banking estimates, meaning when businesses do fall victim, they are losing more money.

> *"By making sure you dial out to verify details using the trusted contact information you have on file, you're less likely to be manipulated by a call placed to you by a fraudster. Answering the phone isn't a proper callback."*
>
> Eric Huber, Fraud Strategy Manager, Commercial Banking

THE FORECAST

Criminals will get more sophisticated in their efforts to avoid detection when attempting BEC—sometimes by compromising more than an email address. They've already started to utilize deepfake technology to impersonate executives' voices on phone calls and even their likenesses over video to add an air of legitimacy to their attacks. As deepfakes become more lifelike, phone calls, video chats and other forms of communication will be more vulnerable to abuse.

continued on next page >

Nobody is immune

Businesses in every region of the country and across every industry have reported attacks. Cybercriminals don't care about your physical address. If you've got an IP address, you're a target.

> *"Fraud is not a region-specific issue. Cybercriminals follow people, money and vulnerable technology—not geography."*
>
> John Geronimo, Executive Director and Fraud Strategy Director, Commercial Banking

THE FORECAST

We expect industry groups and the public sector to ramp up efforts to coordinate their fraud and cybercrime prevention strategies, especially ones focused on protecting critical infrastructure and supply chains. While we don't know where the next hotspot will appear, we do know criminals are constantly improving their methods to launch attacks. To amplify their efforts, criminals use malware or internet bots to do their dirty work. Bots roam the internet looking for unguarded data and system vulnerabilities to launch malicious attacks that allow an attacker to remotely take control of computer systems.

You've got resources to fight back

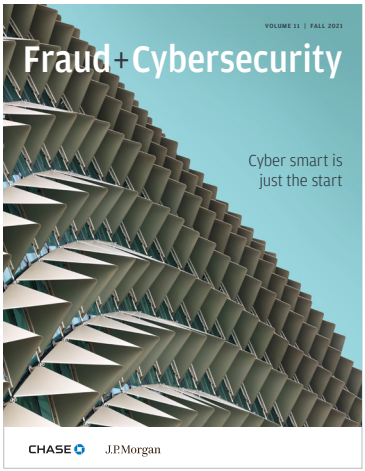
The fight against fraud is constantly evolving. As financial institutions and clients—as well as law enforcement—improve controls and counter-fraud measures, criminals will adapt and escalate in new ways. But the fundamentals of cybersecurity remain the same: Study the threats, follow your controls and ensure your entire team is vigilant. The majority of money lost to BEC schemes by Commercial Banking clients in the first half of 2021 were flagged as irregular by bank control and released by clients.

> *"The common denominator for these attacks is the same: human nature and an overreliance on email. In those cases, a proper callback could have stopped the fraud attempts cold."*
>
> Krysta Gnidziejko, Fraud Strategy Associate, Commercial Banking

Key takeaway

- JPMorgan Chase will continue to research and present the latest advice on how to protect your business. Ready to take action? **Download our BEC Guide.**

The previous article is an excerpt from Fraud + Cybersecurity Magazine: Fall 2021.



DOWNLOAD