DATA SHEET

Check Fraud Prevention

Flag stolen, synthetic, and forged checks well ahead of deposit. Stay one step ahead of fraudsters by tapping into real-time Dark Web intelligence.

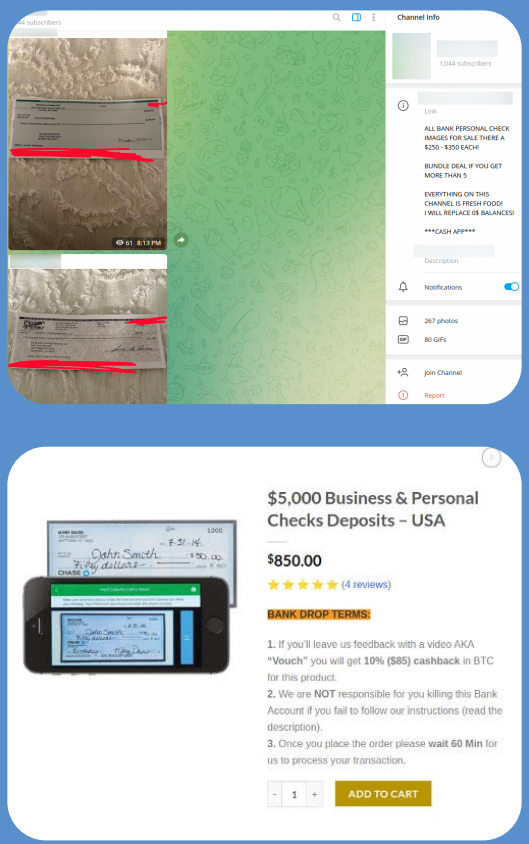
THE CHALLENGE

Recently, financial institutions have been facing a massive spike in check fraud attacks, driving fraud losses sharply upwards. Contributing factors include new check fraud tactics, easy access to check printing software, the growth of remote and mobile deposit channels, ever-improving social engineering schemes, and the increased targeting of postal service employees and facilities.

USING THE DARK WEB TO YOUR ADVANTAGE

Many fraudsters and cybercriminals regularly collaborate and transact on the Dark Web and other "underground" channels. In line with the rapid growth of check fraud, the vast Dark Web ecosystem of financial crimes now includes established communities, vendors, and marketplaces dedicated to check fraud. And they are only getting bigger.

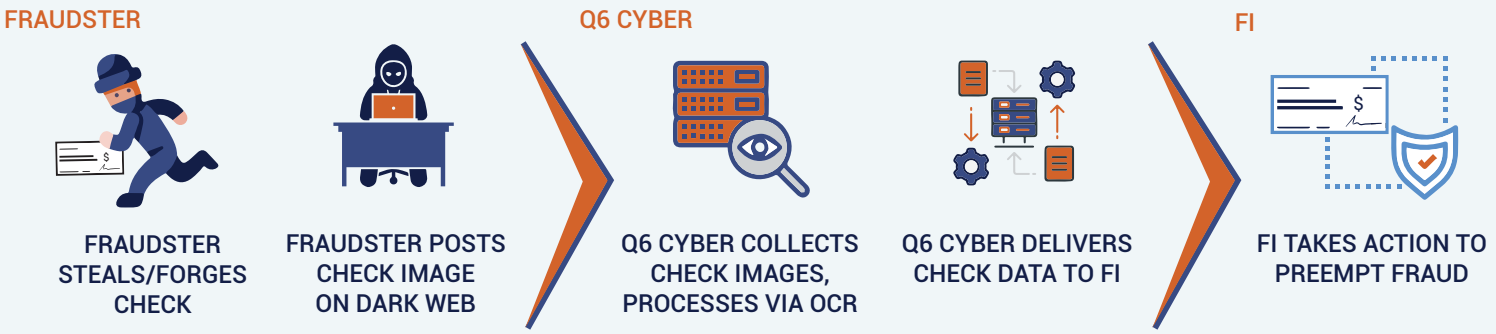
But all this activity on the Dark Web may actually be useful for financial institutions. What if you can leverage comprehensive, real-time Dark Web Monitoring to proactively identify stolen, synthetic, and forged checks ***before*** deposit? Through 24x7 coverage of the Deep & Dark Web and other underground sources, we observe such check images by the hundreds or thousands on a weekly basis. These checks are advertised for sale by malicious actors to fraudsters, and therefore, our intelligence precedes the actual check fraud attempt by hours, days, and even weeks.



Dark Web vendors of stolen checks

PROACTIVELY FLAGGING CHECK FRAUD

Our real-time Dark Web intelligence enables financial institutions to flag specific checks and accounts that are at elevated risk of experiencing fraud. Rather than calculating a risk score at the time of deposit based on a narrow set of indicators, we proactively alert on specific checks that we know to be compromised in some fashion, allowing you to initiate highly targeted fraud mitigation. For example, as the drawing bank, consider placing a stop or extended hold on the check. With the account holder's information compromised and the prevalence of check printing software on the Dark Web, you may want to proactively shut down the account altogether and open a new one. Similarly, as the depositing bank, consider placing extended hold on a check that is known to have been recently compromised.



KEY BENEFITS

- Substantially reduce check fraud
- Stay ahead of fraudsters
- Optimize manual reviews and operational costs
- Avoid customer friction
- Transform check fraud operations from reactive to proactive

CASE STUDIES

$25,000

Check was stolen and posted for sale on an underground channel just two days after it was written. Q6 Cyber collected the check image and reported it to the drawing bank. The bank immediately stopped the check and engaged the account holder to prevent other potential account fraud.

$500,000

Estimated fraud loss savings over a 1-month period for a tier-1 bank. Q6 Cyber collected approximately 300 compromised check images posted on various Dark Web channels and delivered to the bank in near real-time.

ABOUT US

Q6 Cyber is the leading provider of e-crime intelligence to financial institutions worldwide. Q6 Cyber monitors the "Digital Underground" – including the DarkWeb, DeepWeb, malware networks, fraud and cybercrime infrastructure - to proactively identify threats before they materialize into fraud losses and other financial crimes. The company's targeted intelligence produces high ROI through significant reduction of account takeovers, payment card fraud, and many other financial crimes. **Learn more at www.q6cyber.com**

CYBER

Let us help you reinvent the way you manage check fraud.

Contact one of our experts to find out more at

info@q6cyber.com