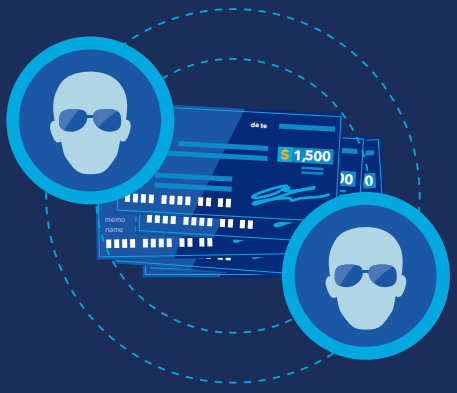
MONITORING CRIMINAL CHANNELS TO FIGHT CHECK FRAUD

The dark web — essentially a hidden part of the internet — is a place criminals can go to further their illicit schemes. Criminals use these hidden websites, as well as online messaging channels, to collaborate with other criminals and sell stolen data in underground marketplaces. Financial institutions may find that monitoring the dark web and secure messaging platforms can provide insights to help them combat check fraud.

THE DARK WEB AND MESSAGING PLATFORMS FACILITATE CHECK FRAUD

Secure messaging platforms and sites hosted on the dark web — which are not discoverable by search engines — create hidden and often-anonymous places for criminal activity, including:

- Selling stolen checks and compromised account information
- Offering forgery kits and templates that can be used to create fraudulent checks
- Sharing vulnerability exploits and playbooks on how to commit check fraud
- Fraud-as-a-Service — criminals who can be hired to create fraudulent checks or commit fraud



EXAMPLE

Two criminals worked together to steal high-value business checks from the mail. They sold the stolen checks via an illicit online marketplace hosted on a secure messaging channel. Other criminals purchased the stolen checks, created counterfeit copies and cashed them at financial institutions. The total value of the stolen checks posted to the secure messaging channel was almost $20 million.

MONITORING CRIMINAL CHANNELS TO FIGHT CHECK FRAUD

CRIMINAL INTELLIGENCE CAN HELP FIGHT CHECK FRAUD

While criminals continue to use these underground spaces to further their illicit activity, these channels also can offer key insights for fraud prevention teams.

Identification and validation of emerging tactics. Monitoring active discussion forums on check fraud can provide insights on the techniques criminals are using to wash and alter checks, forge signatures and create counterfeit checks. Criminals also may share vulnerabilities at specific financial institutions or new tools or methods that have higher success rates. This information can help inform fraud prevention strategies.

Compromised checks, accounts and customer information. Marketplaces on the dark web and online messaging channels may provide specific details about compromised checks, deposit accounts and customers. Identifying this compromised information before fraud occurs can help fraud prevention teams proactively protect customers and their accounts.

Organized crime rings and connections. Identifying bad actors associated with check fraud allows for ongoing monitoring of compromised information and schemes. Intelligence found on the dark web can make connections to other fraud types involving money mules, synthetic identities and new account fraud schemes that help facilitate check fraud.

INCORPORATING INTELLIGENCE TO PREVENT FRAUD

Fraud prevention experts should consider incorporating intelligence from the dark web and secure messaging platforms into their prevention strategies and tools by:

- Establishing what type of intelligence would be most meaningful and actionable — including relevant key words and institution-specific information, such as the name and website of your financial institution.
- Collaborating with internal or external stakeholders to quickly share findings by creating actionable alerts.
- Creating a plan to respond and track the various types of intelligence, once identified. This can be used to identify trends and potential crime rings that may be targeting your institution.

MONITORING CRIMINAL CHANNELS TO FIGHT CHECK FRAUD

CONCLUSION

Check fraud prevention benefits from gathering insights and signals from multiple sources, including the dark web and secure messaging platforms, to enable earlier detection and create a more holistic understanding of the threat landscape. Ongoing monitoring of these criminal resources may help financial institutions reduce losses, protect customers and stay aware of evolving criminal methods. Even in cases where compromised checks are not identified until after fraud occurred, there may be compromised information or insights — such as the possible origin of the compromise or fraud scheme — that can be used to help mitigate vulnerabilities.

The check fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about check fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.