OI CYBERA

CYBERCRIME WATCHLIST™

Minimize costs, loss & regulatory risk - prevent transacting with mule accounts

No matter your industry, organized crime groups (OCGs) are seeking ways to exploit you and your customers. The scale is staggering with the level of non-plastic frauds, especially authorized frauds, growing at a breakneck pace.

The FBI's 2021 IC3 Fraud report[1] showed non-plastic frauds, such as investment frauds, totalled over **$7.5bn**, and in the UK remote payment frauds and authorised frauds reached **£488m**[2] in the first half of 2021 alone. In both cases these were steep increases from previous years.

As customer impact and operational costs of dealing with these complex frauds is high, it is key to target prevention as well as cure, even where there is no legal liability. The common thread with all of these is mule accounts. With many accounts used in the majority of frauds, they are often re-used multiple times before they are closed. So, how do you protect both your customers and your own organization from transacting with mule accounts?

Introducing **CYBERCRIME WATCHLIST™** - a unique and powerful global dataset. Compiled from reported frauds made by victims, financial institutions and law enforcement partners via **CYBERCRIME COMPLAINT™**. With multiple data points, including account and wallet details, this real-time API allows you block known mules throughout the customer lifecycle.

CYBERCRIME WATCHLIST™
benefits you and your customers:

- Lower fraud losses
- Lower operational costs from mules
- Lower False Positive Rates, meaning fewer customers are impacted
- Help meet your regulatory obligations & improved reputation

CYBERCRIME WATCHLIST™
data points[3] for money laundering mule accounts:

- Bank accounts (IBANs)
- Crypto wallet addresses
- URLs (websites)
- Names & users
- Email addresses
- Phone numbers
- Cross-matches

CYBERCRIME WATCHLIST™
supports multiple use cases:

- **Onboarding / KYC** - stop onboarding known mules
- **ODD / mule detection** - identify accounts to close before you and your customers are abused
- **Outbound payments** - stop fraudulent payments in real time
- **Inbound payments** - freezes proceeds of crime as they enter your organization allowing greater repatriation of funds to victims and reducing constructive trustee legal risks

CYBERCRIME WATCHLIST™ a unique, easy to integrate, real-time REST API to reduce fraud across multple-use cases. **CYBERCRIME WATCHLIST™** compliments any existing fraud prevention strategy, as even the best AI needs to be fed 'bads' to promote further learning. **CYBERCRIME WATCHLIST™** is priced based on the volume of API calls, with fixed band prices to aid budgeting.

Add **CYBERCRIME COMPLAINT™** has multiple tiers, with the free 'Partner' tier supporting reporting for your customers & AML alerts – we believe it's the 'right thing' to help disrupt organized criminality and help victims of fraud. Premium & Enterprise tiers* provide additional features such as a dashboard of all your customers' reports, victim support & valuable analysis for your fraud strategy and builds the case for investment in further prevention tools, such as **CYBERCRIME WATCHLIST™.**

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[2] https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf
[3] Further data points are under development
*Monthly subscription

Contact us at mail@cybera.io
Visit our website at www.cybera.io