

A black and white image of a circuit board. In the center, there is a glowing padlock with a key inserted into it. The padlock is illuminated from within, creating a bright, starburst-like effect. The circuit board has a complex pattern of lines and circles, representing electronic components and connections.

Cyber Security ?

A black and white image showing several US dollar bills hanging from a string. The bills are held in place by wooden clothespins. The bills are slightly crumpled and appear to be drying or hanging for display. The background is dark, making the lighter-colored bills stand out.

Anti-Money laundering ?

Financial crime and fraud in the age of cybersecurity

the World Economic Forum noted that fraud and financial crime was a trillion-dollar industry, reporting that private companies spent approximately \$8.2 billion on anti-money laundering (AML) controls alone in 2017. The crimes themselves, detected and undetected, have become more numerous and costly than ever.

As cybersecurity threats compound the risks of financial crime and fraud, institutions are crossing functional boundaries to enable collaborative resistance.

In 2018, the World Economic Forum noted that fraud and financial crime was a trillion-dollar industry, reporting that private companies spent approximately \$8.2 billion on anti-money laundering (AML) controls alone in 2017. The crimes themselves, detected and undetected, have become more numerous and costly than ever. In a widely cited estimate, for every dollar of fraud institutions lose nearly three dollars, once associated costs are added to the fraud loss itself.^[1] Risks for banks arise from diverse factors, including vulnerabilities to fraud and financial crime inherent in automation and digitization, massive growth in transaction volumes, and the greater integration of financial systems within countries and internationally. Cybercrime and malicious hacking have also intensified. In the domain of financial crime, meanwhile, regulators continually revise rules, increasingly to account for illegal trafficking and money laundering, and governments have ratcheted up the use of economic sanctions, targeting countries, public and private entities, and even individuals. Institutions are finding that their existing approaches to fighting such crimes cannot satisfactorily handle the many threats and burdens. For this reason, leaders are transforming their operating models to obtain a holistic view of the evolving landscape of financial crime. This view becomes the starting point of efficient and effective management of fraud risk.

Crime pathways are converging, blurring traditional distinctions Among cyber breaches, fraud, and financial crimes.



Fraud and insider threats

- Internal and external threats
- Retail and nonretail threats
- Insider threats
- Market abuse and misbehavior



Cyber breaches

- Confidentiality
- Integrity
- Systems
- Availability



Financial crimes

- Money laundering
- Bribery and corruption
- Tax evasion and tax fraud

Example : cyberattack on a central bank

Bank employee's **SWIFT** credentials stolen with the help of insiders

Malware surreptitiously installed on the bank's computers to prevent discovery of withdrawals

Funds routed from bank's account at a branch of another country's central bank to a third bank (on a weekend to ensure staff absence)

Withdrawals were made at the third bank through multiple transactions that were not blocked until too late

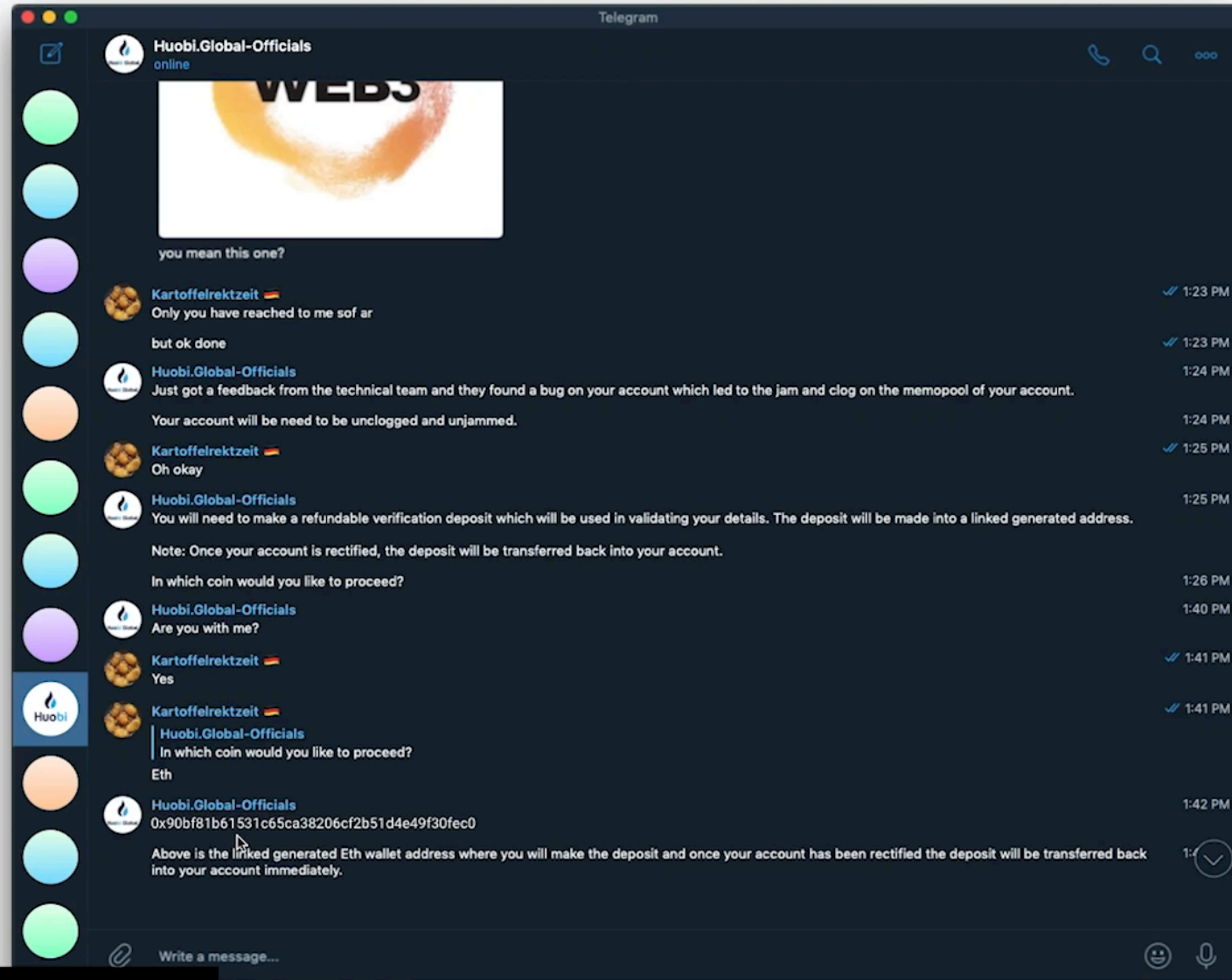
Attacks may have been linked to a known sanctioned entity

SWIFT

Society for Worldwide interbank Financial Telecommunication.

At their core, all functions perform the same three roles using Similar data and processes.

	Identification: “Who is my customer?”	Monitoring: “What transactions are legitimate?”	Response: “How do I respond to a threat?”
Financial crime	<ul style="list-style-type: none"> • Client risk rating • Client due diligence; enhanced due diligence 	<ul style="list-style-type: none"> • Transaction monitoring • Name screening • Payments screening 	<ul style="list-style-type: none"> • Suspicious-activity monitoring • Financial intelligence unit • List management • Do not bank
Fraud	<ul style="list-style-type: none"> • Identity verification, including digital And nondigital presence 	<ul style="list-style-type: none"> • Transaction monitoring and decision making • Device and voice analytics 	<ul style="list-style-type: none"> • Investigations and resolutions teams
Cybersecurity	<ul style="list-style-type: none"> • Credentials management 	<ul style="list-style-type: none"> • Security-operations center • (SOC) and network-operations center, which enable monitoring 	<ul style="list-style-type: none"> • SOC • Forensics • Resolution teams
Synergies across functions	<ul style="list-style-type: none"> • Risk scoring of customers using common and similar customer data, such as financials, digital footprint, nondigital records 	<ul style="list-style-type: none"> • Risk scoring of transactions using similar Analytics and common use cases based on timing, destination, source,value and frequency, device, and geolocation intelligence 	<ul style="list-style-type: none"> • Common feedback loop to develop a holistic view on modus operandi and drive top-down use-case development • Pooling of resources and capabilities

**Case 1 : Fake telegram account**

A stack of three gold Bitcoin coins is positioned in the center-left of the frame. The top coin is clearly visible, showing the Bitcoin symbol and the words "BITCOIN" and "DECENTRALIZED DIGITAL CURRENCY". The coins are resting on a US dollar bill, with the portrait of George Washington and the words "ONE DOLLAR" and "UNITED STATES OF AMERICA" visible. In the background, a computer keyboard is partially visible, with keys like "Alt Gr" and a function key with a cursor icon discernible. The entire image has a dark, muted color palette, giving it a serious and somewhat somber feel.

No Money for Terror.





A photograph of four men standing in front of a large white banner. The man on the far left is of Asian descent, wearing a dark suit jacket over a light blue button-down shirt and dark trousers. The second man from the left is bald, wearing a grey suit jacket, a pink shirt, and a red tie. The third man is of Asian descent, wearing a dark blazer over a black polo shirt and light-colored trousers. The man on the far right is of European descent, wearing a dark suit jacket, a light blue shirt, and a striped tie. All four men are wearing blue lanyards with identification badges. To the left of the men is a red flag with a yellow star. The background features a wood-paneled wall and a modern architectural structure with grey panels.

NO MONEY FOR TERROR

Ministerial Conference on Counter-Terrorism Financing

AUSTRALIA

Cyber Security = Cyber Anti-Money laundering

Digital Financial Crime and relevant anti money laundering should be addressed under **Cyber Security perspective** in a way of efficiency.

uppsala security