



KOBRE & KIM | DISPUTES
AND INVESTIGATIONS

AMERICAS | NEW YORK . CHICAGO . DELAWARE . MIAMI . SAN FRANCISCO . SÃO PAULO . WASHINGTON DC

APAC | HONG KONG . SEOUL . SHANGHAI

CARIBBEAN | BVI . CAYMAN ISLANDS

EMEA | CYPRUS . DUBAI . LONDON . TEL AVIV

Reverse Engineering the Bitfinex Case

Andrew Stafford QC

The International Academy for Financial Crime
Litigators | 15 July 2022



AGENDA

1

On the Trail of Dutch Lichtenstein and Razzlekhan

Reverse Engineering the DOJ's Tracing and Seizure of Stolen Bitcoin from Bitfinex

2

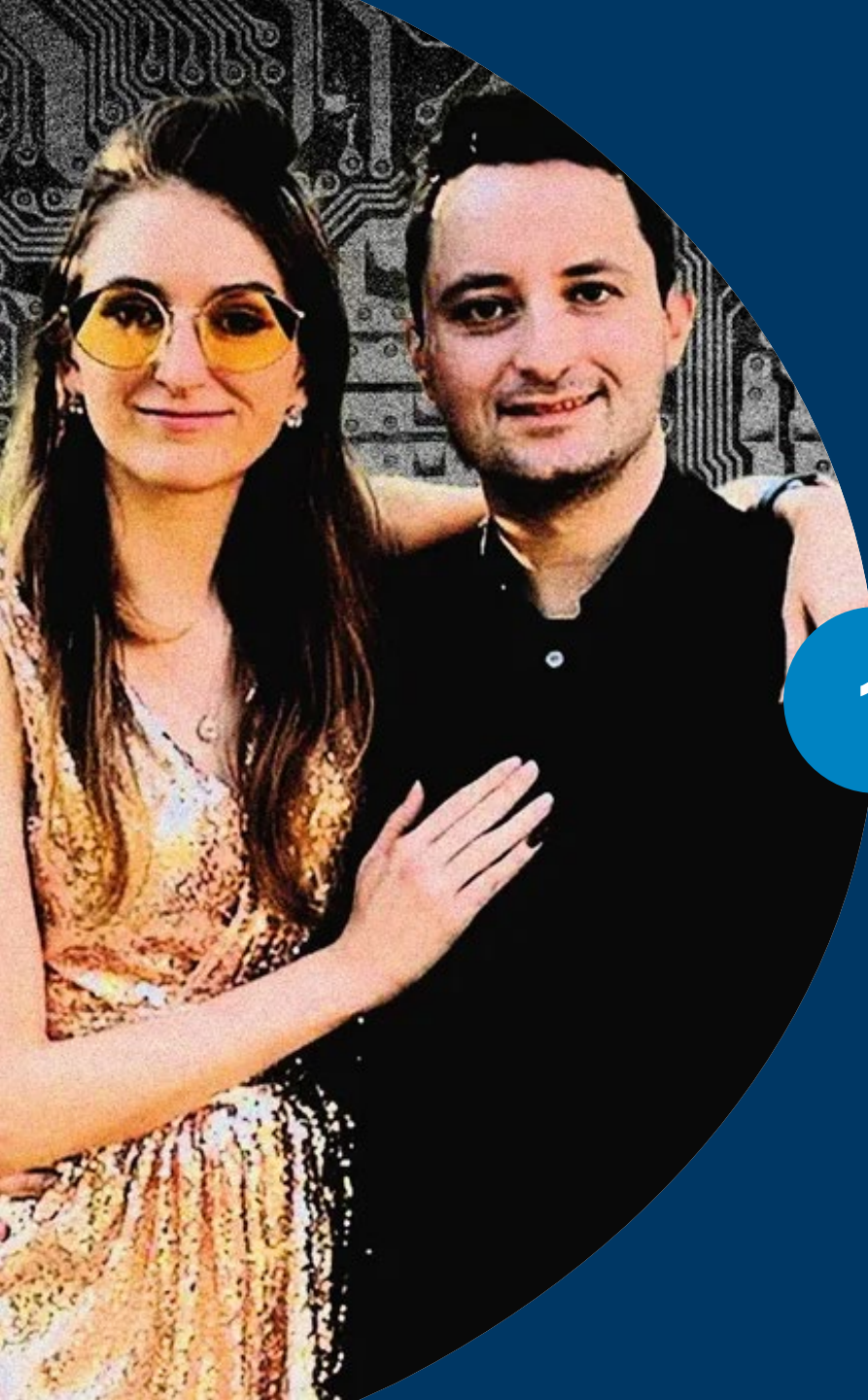
Case Law Development

Creating more clarity?

3

Unorthodox Methods of Service

Email, Websites, and Social Media



1

On the Trail of Dutch Lichtenstein and Razzlekhan

On the Trail of Dutch Lichtenstein and Razzlekhan

- Ilya Lichtenstein and Heather Morgan are a married couple who went by the self-styled monikers Dutch Lichtenstein and Razzlekhan.
- Dutch and Razzlekhan worked by day, as a blockchain start-up founder and a tech company CEO respectively. By night, they were an aspiring magician and rapper.



On the Trail of Dutch Lichtenstein and Razzlekhan

- In August 2016, a hacker successfully initiated over 2,000 unauthorized transactions, in which approximately 120,000 BTC was transferred from Bitfinex to an outside wallet.
- At the time of the breach, this was valued at approximately USD \$71 million. As of February 2022, the stolen funds were valued at over USD \$4.5 billion.
- Dutch and Razzlkahn are accused of laundering the bitcoin through a darknet labyrinth that took the combined efforts of the FBI, DHS, and IRS to unravel. For the laundering, they allegedly took various steps including:
 - Using accounts set up with fictitious identities;
 - Moving stolen funds in a series of small amounts;
 - Utilizing computer programs to automate transactions;
 - Layering stolen funds by depositing them in exchanges and darknet markets;
 - Converting the Bitcoin to other forms of virtual currency (chain-hopping); and
 - Using US-based business accounts to legitimize activity.

On the Trail of Dutch Lichtenstein and Razzlekhan

Department of Justice


Office of Public Affairs

FOR IMMEDIATE RELEASE

Tuesday, February 8, 2022

Two Arrested for Alleged Conspiracy to Launder \$4.5 Billion in Stolen Cryptocurrency

Government Seized \$3.6 Billion in Stolen Cryptocurrency Directly Linked to 2016 Hack of Virtual Currency Exchange

View Deputy Attorney General Monaco's Remarks [here](#). 

Two individuals were arrested this morning in Manhattan for an alleged conspiracy to launder cryptocurrency that was stolen during the 2016 hack of Bitfinex, a virtual currency exchange, presently valued at approximately \$4.5 billion. Thus far, law enforcement has seized over \$3.6 billion in cryptocurrency linked to that hack.

"Today's arrests, and the department's largest financial seizure ever, show that cryptocurrency is not a safe haven for criminals," said Deputy Attorney General Lisa O. Monaco. "In a futile effort to maintain digital anonymity, the defendants laundered stolen funds through a labyrinth of cryptocurrency transactions. Thanks to the meticulous work of law enforcement, the department once again showed how it can and will follow the money, no matter what form it takes."

"Today, federal law enforcement demonstrates once again that we can follow money through the blockchain, and that we will not allow cryptocurrency to be a safe haven for money laundering or a zone of lawlessness within our financial system," said Assistant Attorney General Kenneth A. Polite Jr. of the Justice Department's Criminal Division. "The arrests today show that we will take a firm stand against those who allegedly try to use virtual currencies for criminal purposes."

On the Trail of Dutch Lichtenstein and Razzlekhan

What the DOJ did

1. Traced the flow of stolen cryptocurrency on blockchain(s), including through a darkweb website, AlphaBay.
2. Obtained useful disclosure information from third party intermediaries including crypto-exchanges and traditional banks. This information included common Know-Your-Client records, such as email and home addresses, drivers licenses, account opening documentation, and internet protocol information.
3. Obtained a search warrant to access defendants' documents and other content stored in a cloud-based account and served that warrant upon the cloud service provider.
4. Decrypted the encrypted files stored in the cloud account.
5. Locked down the identified assets.

On the Trail of Dutch Lichtenstein and Razzlekhan

What the US DOJ did	What Litigators can do to replicate that action
<p>1. Traced the flow of stolen cryptocurrency on blockchain(s)...</p>	<p>Litigators generally can replicate this tracing through the Chainalysis Reactor software we use in-house.</p> <p>Reactor is a powerful tool through which we can see and analyze inflow and outflow transactions to and from identified digital wallets. If we have one digital wallet address to start with, we can usually trace the flow of the cryptocurrency, and create easy to read diagrams useful for narratives and presentations.</p> <p>There are some limits to this software, however. For example, bad actors often will use various techniques (e.g., use of darkweb, mixers, peel chain, and privacy coins) to obfuscate their transaction trail.</p>

On the Trail of Dutch Lichtenstein and Razzlekhan

What the US DOJ did	What Litigators can do to replicate that action
2. Obtained useful disclosure from third party intermediaries...	<p>Litigators can seek similar disclosures from third parties depending on the jurisdiction. For example:</p> <p>First, we can try a demand letter to third parties seeking voluntary compliance; and</p> <p>Second, we can seek third party disclosures consistent with local laws e.g. third party subpoenas in the U.S. and Norwich Pharmacal or Bankers Trust applications in English common law jurisdictions.</p> <p>NB options to obtain discovery in support of proceedings aimed at unknown defendants (i.e., John Doe or Persons Unknown actions in the U.S. or English common law jurisdictions, respectively).</p>

On the Trail of Dutch Lichtenstein and Razzlekhan

What the US DOJ did	What Litigators can do to replicate that action
3. Obtained a search warrant to access defendants' documents and other content...	<p>This one is difficult for us to <i>replicate</i> civilly.</p> <p>But the Anton Piller jurisdiction (ie search and seizure) can, in the right case, afford analogous access to a defendant's data/documents.</p> <p>In the context of crypto assets, such an order was indeed granted in a Canadian case in connection with the alleged theft of \$15 million in digital assets from the plaintiff's digital wallet.</p> <p><i>Cicada 137 LLC v. Medjedovic</i>, 2021 ONSC 8581 (<i>Cicada 137</i>)</p> <p>The likely utility of this will be limited by the fact that an Anton Piller order does depend on jurisdictional reach of the court granting an order – it will not make a search and seizure order to be executed outside its' home turf.</p>

On the Trail of Dutch Lichtenstein and Razzlekhan

What the US DOJ did	What Litigators can do to replicate that action
<p>4. Decrypted the encrypted files stored in the cloud account.</p>	<p>This depends on the level of decryption necessary.</p> <p>Assuming we have appropriate access to the documents, we can try to use open-source tools to crack passwords, particularly if using a computer with high processing capabilities. There may be vendors who can assist as well.</p>

On the Trail of Dutch Lichtenstein and Razzlekhan

What the US DOJ did	What Litigators can do to replicate that action
5. Locked down the identified assets.	<p>Freezing orders can be obtained to lock down the identified assets</p> <ul style="list-style-type: none">• Can be worldwide• Can include valuable ancillary orders (e.g. discovery orders against third parties), especially valuable when the identity of the bad actor is at the time unknown.• Can extend the extra-territorial reach of Norwich Pharmacal orders• Can be directed to “Persons Unknown”• Can be granted in aid of foreign proceedings – <i>Broad Idea v Convoy Collateral Ltd</i> [2021] UKSC 24



2

Case Law Development

Case Law Development

- Blockchain and cryptocurrencies are classified as property. This is the important key which unlocks equity's capacity to determine that the fruits of fraud are held on trust for the victim, and to impose tracing orders.
 - *AA v Persons Unknown* [2019] EWHC 3556 (Comm)
- The *lex situs* of cryptocurrency is the place where the person or company who owns it is domiciled. Important for establishing jurisdiction grasp of the court.
 - *Ion Science v Persons Unknown* (unreported) (21 December 2020)
- The private key for a cryptocurrency is confidential information (thus creating another potential cause of action).
 - *Fetch.AI Ltd & Anor v Persons Unknown Category A & Ors* [2021] EWHC 2254 (Comm)
- Orders for third party disclosure can be obtained against cryptocurrency exchanges in support of actions for loss arising out of cryptocurrency fraud.
 - *Fetch.AI Ltd*

Case Law Development

- The court refused to permit a claimant to provide security for costs in the form of cryptocurrency, but may have to grapple with the problem for fortification of a freezing order
Tulip Trading v Bitcoin Association for BSV [2022] EWHC 141 (Ch)
Yu Ying v Leung Wing Hei [\[2022\] HKCFI 1660](#).
- The European Parliament reached a provisional deal on a new bill extending the "travel rule" in traditional finance to crypto-assets service providers (CASPs).
 - Ensuring crypto-assets can be traced in the same way as traditional money transfers.
 - Limited to money laundering and terrorism issues.
 - Could therefore become part of the strategic judgment – criminal or civil recovery strategy?
 - <https://www.europarl.europa.eu/news/en/press-room/20220627IPR33919/crypto-assets-deal-on-new-rules-to-stop-illicit-flows-in-the-eu>



3

Unorthodox Methods of Service

Unorthodox Methods of Service

▪ Email & Text

- Service by **email** in civil matters *Bacon v Automattic Inc* [2012] 1 W.L.R. 753.
- Service of injunction by text *NPV v QEL and another* [2018] EWHC 703 (QB).

▪ Social Media

- *Gray v Hurley* [2019] EWHC 1636 (QB) the court allowed service of the claim form by **WhatsApp** message.
- *CMOC v Persons Unknown* [2017] EWHC 3599 (Comm). – via **Facebook**
 - Also, **Facebook service** permitted in NZ (Axe Market Gardens); Canada (Knott Estate); Australia (MKM Capital Pty).
- *Pirtek (UK) Ltd v Jackson* [2017] EWHC 2834 (QB) service via a section of a **website** associated with the defendant called “Contact Bob”.
- **Twitter** has also been permitted by a UK judge *Blaney v Persons Unknown* (October 2009).

Unorthodox Methods of Service

- Unorthodox methods of service elsewhere
 - **USA**
 - In *K.A. v. J.L.*, 450 N.J. Super. 247 (Ch. Div. 2016), plaintiffs were permitted to serve process on a defendant through **Facebook**.
 - *Wimbledon Fin. Master Fund, Ltd. v Weston Capital Mgt. LLC* 2017 NY Slip Op 31961(U), 'alternative service' was permitted through the court's own **electronic filing system** (the NYSCEF system).
 - *LCX AG vs. John Doe Nos. 1-25* - service via **NFT / blockchain** linking to a website.
 - **Singapore**
 - In *David Ian Andrew Storey v. Planet Arkadia Pte Ltd & 2 others* [2016] SGHCR 7, the Court granted an application for substituted service "through **email, Skype, Facebook** and an **Internet Message Board**".
 - **India**
 - Starting in 2016, the Indian High Court has approved service by **WhatsApp**. Example case: *Tata Sons Limited & Ors v John Doe(s) & Ors* [2016].

Unorthodox Methods of Service

- **Hong Kong**
 - *Hwang v Golden Electronics Inc* [2020] HKCFI 1084, 9 June 2020 - service via **data room**.
- **Nigeria**
 - In *Mohammad Awwaldanlami, Esq. v Governor of Taraba State & 24 Ors* (Suit No: TRST/11/2018, Motion No: TRST/67M/18), the Court allowed for service by “posting and sharing on **social media**.”



KOBRE & KIM | DISPUTES
AND INVESTIGATIONS

Thank you

AMERICAS | NEW YORK . CHICAGO . DELAWARE . MIAMI . SAN FRANCISCO . SÃO PAULO . WASHINGTON DC

APAC | HONG KONG . SEOUL . SHANGHAI

CARIBBEAN | BVI . CAYMAN ISLANDS

EMEA | CYPRUS . DUBAI . LONDON . TEL AVIV