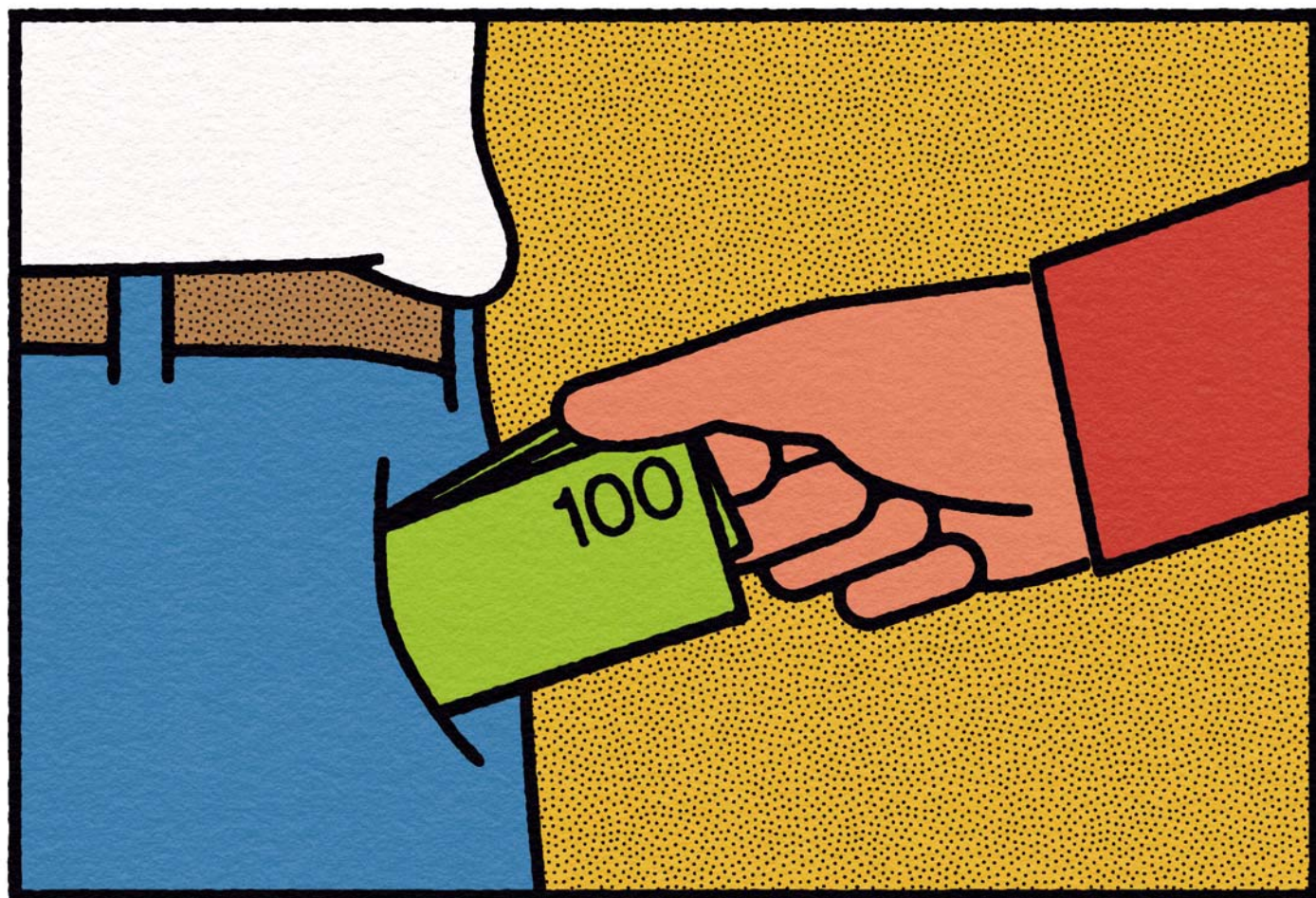


# Doppelt

Windige Tauschangebote, geklonte Unternehmen:  
Dubiose Banden bieten Anlegern an,  
verloren gegangenes Geld zurückzuholen. Woran  
man solche Recovery Scams erkennt

TEXT  
Saskia Littmann



# verzockt

**D**as Angebot, das der freundliche Herr Hahn da am Telefon unterbreitete, klang vielversprechend: „Wir helfen Ihnen dabei, dass Sie Ihr Geld schon in kurzer Zeit wiederhaben.“ Wolfgang Wagner wollte das nur zu gerne glauben. Anfang 2017 hatte der heute 85-Jährige rund 10 000 Euro in Mittelsstandsanleihen der ClinicAll Germany investiert. Sechs Prozent Zinsen hätten die Papiere regelmäßig abwerfen sollen, mit dem Geld wollte Wagner, der eigentlich

anders heißt, seine Rente aufbessern. Daraus ist nichts geworden.

Zweimal kassierte er Zinsen für seine Anteile. Danach, im September 2019, ging ClinicAll Germany pleite. Wagners zusätzliche Einnahmequelle fürs Alter schien ausgetrocknet – bis Herr Hahn anrief. Der machte ihm ein lukratives Tauschangebot. Wagner könne seine nahezu wertlosen Anleihen in Aktien des britischen Pharmakonzerns AstraZeneca tauschen. Er bekomme diese zu einem günstigen Preis, zahle weniger als den aktuellen Kurs.

Sobald er bezahlt habe, würden die Papiere weiterverkauft. Insgesamt kriege

Wagner sein gesamtes Geld zurück – nicht nur die Kosten für die Aktien, sondern auch die verloren geglaubten 10 000 Euro aus dem Anleiheinvestment. Denn AstraZeneca, so erklärt es Hahn, sei an den Daten der ClinicAll interessiert und unterbreite deshalb dieses gute Angebot. Sein Unternehmen, die Conafor Finance AG, sei der Vermittler des Tauschs.

Kurzzeitig sah es für Wagner so aus, als könne er seine Rente doch noch aufbessern. Mit etwas Geld aus einem Hausverkauf konnte er den Aktienkauf gerade so stemmen. Ende Oktober 2023, wenige Wochen nach dem ersten Telefonat mit ▶

Herrn Hahn, erhielt Wagner dann auch die Bestätigung über das Tauschgeschäft. Auf einem mit diversen TÜV-Siegeln und Logos versehenen Papier bestätigt Patrick Müller, seines Zeichens Chief Executive Officer der Conafor Finance, dass Wagner 100 AstraZeneca-Aktien gekauft hat, für 119 Euro das Stück. Nach dem außerbörslichen Weiterverkauf der Papiere werde die Conafor Finance ihm „binnen 48 Stunden“ 23 800 Euro auf sein Konto erstatten – 1900 Euro mehr, als Wagner insgesamt investiert hat.

Das Geld ist nie auf seinem Konto bei der heimischen Sparkasse angekommen. Seine Versuche, die Conafor Finance oder Herrn Hahn telefonisch oder per Mail zu erreichen, sind alle gescheitert.

## ORGANISierter RIESENMARKT

Was Wagner passiert ist, nennt sich Recovery Scam, auf Deutsch: Rückgewinnungsbetrug. Betrüger nutzen den Verlust von Anlegern, um ihnen mit der Aussicht auf eine Entschädigung ein zweites Mal Geld aus der Tasche zu ziehen. Bei Wagners Fall handele es sich um eine neue Form dieses Betrugs, erklärt Rechtsanwalt David Ritschel von der Kanzlei Ritschel & Keller – und um eine besonders perfide noch dazu. Denn das Unternehmen Conafor Finance gibt es tatsächlich, die Firma ist im Schweizer Handelsregister eingetragen, ein Patrick Müller ist dort auch Verwaltungsrat. Selbst der auf Anlagebetrug spezialisierte Ritschel räumt ein, dass die Unterlagen der geklonten Conafor Finance sehr echt aussähen. Für Laien seien sie kaum als Betrug zu erkennen.

Fälle wie dieser zeigen, wie professionell Anleger mittlerweile abgezockt werden – auch und gerade mit Recovery Scams. „Die Zahl der Fälle nimmt immer weiter zu“, sagt Anwalt Arthur Wilms von der Kanzlei Herfurtner. Wie Ritschel betreibt auch er viele Mandanten, denen Ähnliches widerfahren ist. Das sei ein „Riesenmarkt“ von vielen Millionen Euro, sagt Wilms. Anleger würden so teilweise sechstellige Summen verlieren.

Das Muster ist immer ähnlich, und zwar so: Nachdem ein Anleger bei einem Investment Geld verloren hat, wird er von den mutmaßlichen Betrügern kontaktiert. Sie geben sich als Kanzlei, Unternehmen oder Finanzaufsicht aus, kopieren deren Webseiten und bieten an, das verlorene Geld gegen eine Provision wiederzube-

schaffen. Die überweist der Anleger normalerweise auf ein ausländisches Konto. Häufig wird Geld nachgefordert. „Das geht oft so lange, bis die Leute kein Geld mehr haben“, sagt Ritschel. Dann herrscht Funkstille, das Geld ist futsch.

In den meisten Fällen sind die Unglücksraben schon vorher auf einen Betrug reingefallen, etwa auf gefälschte Onlinehandelsplattformen. Dort haben sie häufig Tausende Euro in vermeintliche Kryptowährungen oder Derivate investiert und alles verloren. „Früher“, sagt Anwalt Ritschel, „war nach dem eigentlichen Betrug Schluss.“ Das sei jetzt anders.

Teilweise sei der Schaden sogar höher als beim ursprünglichen Betrug. Mutmaßlich stecken oft dieselben Betrüger hinter der zweiten Tat. Die Daten ihrer Opfer haben sie dann ohnehin schon. Der Schaden reiche von wenigen Tausend bis hin zu mehreren Hunderttausend Euro. „Das richtet sich nach dem ursprünglichen Investment“, sagt Ritschel. Wagner ist vorher keinem anderen Betrug aufgesessen – gefunden haben die Betrüger ihn trotzdem.

Ermittler und Anwälte berichten, wie organisiert die mutmaßlichen Täter dabei vorgehen. Früher fielen viele dubiose Angebote dank E-Mails voller Rechtschreibfehler und schlecht nachgebauter Logos schnell durchs Raster, aber mittlerweile sehen viele davon täuschend echt aus. Normalerweise steckten dahinter gewerbsmäßig organisierte Banden, das Bundeskriminalamt (BKA) spricht von „international agierenden Tätergruppen“. Diese klonen nicht nur eine Webseite, sondern Hunderte. Dank künstlicher Intelligenz geht das einfacher denn je. Oft seien die Banden in verschiedene Abteilungen aufgeteilt: Die einen erstellen die kopierte Webseite, andere koordinieren Zahlungen, wieder andere arbeiten wie eine Art Callcenter, sprechen diver-

se Sprachen und übernehmen die Telefonate mit den potenziellen Opfern.

Dank Datenlecks, Hackerangriffen und Darknet wird es für die Täter immer einfacher, an Daten zu gelangen. Sind die erst mal da, geht alles sehr schnell. So war es auch im Fall der angeblichen Conafor Finance AG. Erst Ende August 2023 wurde die von den mutmaßlichen Betrügern genutzte Webseite [www.conaforfinance.com](http://www.conaforfinance.com) laut Domain-Datenbanken registriert. Kurze Zeit später wurden die Opfer bereits kontaktiert, Ende September erhielt Anleger Wagner die erste Rechnung der falschen Conafor Finance. Die Webseite ist längst nicht mehr erreichbar. Auch Fragen der WirtschaftsWoche ließ das angebliche Unternehmen unbeantwortet.

Genauere Fallzahlen zu Recovery Scams gibt es nicht. Die Finanzaufsicht BaFin warnt generell vor dem Phänomen. Das BKA verweist auf das Bundeslagebild zur Wirtschaftskriminalität von 2022. 3169 Fälle wurden insgesamt als Betrug oder Untreue im Zusammenhang mit Kapitalanlagen polizeilich erfasst. Im Bericht heißt es, dass Geschädigte nach einem Anlagebetrug auf Onlineplattformen „nach Abbruch des Kontakts zu den Tätern und einem somit erlittenen Totalverlust“ häufig „mittels eines sogenannten ‚Recovery Fraud‘ erneut zu Betrugsopfern werden“.

## DIE SPUR FÜHRT NACH ZÜRICH

In wie vielen Fällen die angebliche Conafor Finance erfolgreich agieren konnte, ist offen. Der WirtschaftsWoche sind mehrere Fälle bekannt, teilweise haben Anleger hohe fünfstelligen Beträge verloren. Jedes Mal sollten die Opfer Aktien von AstraZeneca kaufen. Dem britischen Konzern ist diese Art von Betrug bekannt. „Wir warnen unsere Aktionäre in unserem Jahresbericht davor“, heißt es seitens des Unternehmens. Man fordere Betroffene dringend dazu auf, sich bei den zuständigen Aufsichtsbehörden zu melden.

„Die große Frage ist, wie die Betrüger an die Daten der Anleihegläubiger gekommen sind“, sagt Anwalt Ritschel. Mittlerweile ermitteln mindestens drei deutsche Staatsanwaltschaften gegen den angeblichen Patrick Müller beziehungsweise seine Geschäftspartner. Auch die Schweizer Finanzaufsicht Finma warnt davor, das Vehikel nicht mit der im Schweizer Handelsregister eingetragenen echten Conafor Finance AG zu verwechseln.

# 10

PROZENT  
oder mehr der ursprünglich  
investierten Summe verlangen  
die Betrüger für das Zurückholen  
des Geldes

Ob die eigentlich von ihrem Doppelleben weiß? Ein Anruf in Zürich. Telefonisch ist das Unternehmen nicht erreichbar, eine Webseite hat es nicht. Seinen Sitz hat es laut Register in einem schmucken Altbau in einer kleinen Gasse der Zürcher Innenstadt. Ein Zusammenhang zur mutmaßlich betrügerischen Conafor Finance AG lässt sich nicht ausmachen.

„Es ist üblich, dass Täter Handelsregister durchforsten und nach Firmen suchen, die keine Internetpräsenz haben und deren Namen nach Finanzdienstleister klingen“, sagt Anwalt Ritschel. Besonders beliebt seien Firmen aus der Schweiz und Großbritannien. Der Eintrag ins Handelsregister vermittele Seriosität.

## DER PSYCHOFAKTOR

So auch bei Wagner. „Ich habe die sofort gegoogelt, da gab es eine Adresse, das war alles astrein“, sagt der ehemalige Unternehmer, der sich gut mit Finanzen auskennt. Skeptisch wurde Wagner, als Herr Hahn auf seine Anrufe und E-Mails nicht mehr reagierte. Da hatte er das Geld aber schon überwiesen, auf Konten in den USA und den Niederlanden.

Genau wie Fritz Sturm. Der Selbstständige investierte einen Großteil seines für die Rente zurückgelegten Geldes in Anleihen der ClinicAll Germany. Über 130 000 Euro steckte er in die Mittelstandsbonds des Herstellers von digitaler Krankenhaussoftware. Als der Anruf der angeblichen Conafor Finance kam, war Sturm, der ebenfalls anders heißt, in einer schwierigen Lage. In seiner Ehe lief es nicht, er hatte Stress bei der Arbeit. Obwohl er skeptisch war, stimmte er dem Angebot zu. Etwa 75 000 Euro zahlte er, um an das verlorene Geld zu kommen.

„Viele Täter sind für solche psychologischen Aspekte sensibilisiert“, erklärt Anwalt Wilms. Sie teilten ihre potenziellen Opfer in unterschiedliche Kategorien ein. Manche seien wie Sturm emotional anfällig. Andere müsse man stärker unter Druck setzen. Die Opfer seien überwiegend Männer, „jeden Alters und aus allen sozialen Schichten“.

Anders als Wagner und Sturm kaufen Wilms' Mandanten meistens keine Mittelstandsanleihen. Sie legen ihr Ersparnis direkt auf dubiosen, zuweilen betrügerischen Onlinetradingplattformen an. Das Geschäftsmodell dieser Anbieter ist bekannt. Kunden werden anhand von De-



mokontos und oft manipulierten Kursverläufen sagenhafte „Gewinne“ in Aussicht gestellt. Weil es so gut läuft, investieren sie mehr. Den Betrug merken viele erst, wenn sie versuchen, ihre vermeintlichen Gewinne von der Plattform abzuziehen.

Bei der Kontaktaufnahme zum zweiten Betrug gäben sich die mutmaßlichen Täter zum Beispiel als Anwaltskanzlei aus, erklärt Anwalt Wilms. „Teilsweise werden die Opfer noch Jahre später kontaktiert.“

Besonders perfide ist ein relativ neues Phänomen im Zusammenhang mit Kryptowährungen. „Anleger sollen dann die geforderte Gebühr auf eine Kryptowallet eines anderen Kunden einzahlen“, sagt Wilms. Erst dann könnten sie ihr verlorenes Geld wiederbekommen. Die Geschädigten sendeten sich schließlich untereinander Geld hin und her – und hülften so im Zweifel noch bei der Geldwäsche mit. Erst wenn genug Verschleierungsrunden über alle möglichen Wallets gedreht wurden, senden die Betrüger das Geld an ihr eigenes Kryptoportemonnaie.

Für Ermittler sind solche Geldkreisläufe schwer zu durchbrechen, nur wenige deutsche Staatsanwaltschaften arbeiten bisher mit einer Software, die Kryptozahlungen nachverfolgen kann. Fälle wie die von Wagner und Sturm, bei denen das Geld über normale Bankkonten ins Ausland überwiesen wurde, ließen sich dagegen mittels Rechtshilfeersuchen bei den ausländischen Behörden nachverfolgen – aber auch das dauert lange und führt oft

zu keinem Ergebnis. Trotzdem war Wagners Enttäuschung groß, als die Staatsanwaltschaft Magdeburg seinem Anwalt David Ritschel schon kurz nach dessen Anzeige mitteilte, die Ermittlungen einzustellen. Ein Rechtshilfeersuchen verspreche keinen Erfolg, gegen die Beschuldigten „ergeben sich keine weiteren Ermittlungsansätze“, heißt es in einem Schreiben, das der WirtschaftsWoche vorliegt. Mittlerweile wurden die Ermittlungen wieder aufgenommen, sie dauern an.

## TEXTBAUSTEINE GOOGLN

Tatsächlich sind die Täter schwer zu enttarnen. Teilweise schreiben die Betrüger eigene Onlinebewertungen zu selbst manipulierten Handelsplattformen. Darin geben sie sich als Opfer aus und loben die Hilfe eines angeblichen Anwalts. Wer dem Link im vermeintlichen Nutzerkommentar folgt, landet auf einer Kanzleiwebseite – die wiederum gefälscht ist.

Auch die Kanzlei Schlun & Elseven wurde dafür schon missbraucht. „Unsere komplette Seite wurde nachprogrammiert“, erzählt Anwalt Matthias Wurm. Die mutmaßlichen Betrüger nutzten nicht nur das Logo und den Namen der Kanzlei, sie verwendeten auch deren E-Mail-Signaturen. Wurm rät Anlegern, über das Verzeichnis der Bundesrechtsanwaltskammer herauszufinden, ob der Absender ein tatsächlich zugelassener Anwalt ist. Doch selbst dann könnte es sich um eine gestohlene Identität handeln.

Wichtiger denn je ist es deshalb, darauf zu achten, ob eine Webseite ein vernünftiges Impressum hat. Anleger Wagner wäre womöglich skeptisch geworden, hätte er gewisse Formulierungen der angeblichen Conafor Finance in seine Google-Suche eingegeben. „Nichts macht uns glücklicher als zufriedene Kunden“, heißt es in der automatischen E-Mail-Signatur des Unternehmens. Und weiter: „Wir sind uns unserer Verantwortung bewusst, denn sie brauchen einen starken Partner.“ Wer den Textblock in seine Suchmaschine eingibt, landet auf der Webseite einer Schweizer Firma namens DaKya. Sie hat den gleichen Wortlaut auf ihrer Homepage, ein vollständiges Impressum sucht man vergeblich. Laut Schweizer Handelsregister ist DaKya als Finanzdienstleister tätig. Noch ein Klon? Das Unternehmen kann genauso gut echt sein. Ein Schelm, der gleich wieder Böses denkt. ■