ATLAS

GRAPHIKA REPORT

Looking for Love on All the Wrong Pages

Romance Scammers Masquerade as Celebrities and Lonely Singles to Ensnare and Deceive Online Love Seekers

Léa Ronzaud

02.2025

Looking for Love on All the Wrong Pages

Romance Scammers Masquerade as Celebrities and Lonely Singles to Ensnare and Deceive Online Love Seekers

Overview

Romance scams have become a permanent feature in the online fraud landscape, according to financial services and government officials. Losses linked to scams that ensnare internet users in fake relationships and defraud them of their money totaled $1.14 billion in the U.S. in 2023, according to the U.S. Federal Trade Commission. In January 2025, a 53-year-old woman was reportedly tricked out of $855,000 in what she believed was a secret long-term relationship with actor Brad Pitt.

Through our ATLAS intelligence reporting, Graphika regularly detects, tracks, and helps disrupt a wide array of scams on multiple online platforms. Working with industry partners at Meta, we've joined a campaign to raise public awareness about online scams. This report focuses on romance scams ahead of Valentine's Day celebrations in multiple countries.

Our findings are not exhaustive but rather a set of case studies illustrating how these types of scams attempt to engage, deceive, and defraud people of their money. We've selected the examples based on a combination of key attributes, including their relevance as romance scams, prevalence across internet platforms, and notable tactics, techniques, and procedures.

Key Findings

- As seen in our previous reporting on shopping scams, romance scams occur globally. We've observed actors linked to locations in Nigeria and Kenya targeting users from the U.S. to Japan, often tailoring activities to specific target audiences. A network predominantly targeting older U.S. women, for instance, used inauthentic accounts impersonating U.S. military officials, while fake dating scams catering to Southeast Asians and Africans dangled the promise of visas for Western countries.

- These scams span the entire internet, with operators using different web surfaces at different stages in the kill chain. Social media and other public platforms are typically among the channels by which scammers first engage targets before directing them to messaging apps such as Telegram – where they're less likely to be detected and disrupted. There, the

scammers can engage in social engineering and manipulate the target into sending money via wire transfers, gift cards, or cryptocurrency exchanges.

- Impersonation and fake personas are a core component of romance scams, providing a character for the target to build an emotional relationship with. They might be a celebrity or other high-profile public figure, or an ordinary member of the public whose images the scammers use in fake dating posts.
- Although deception and inauthentic behaviors are integral, romance scammers seem to focus on quantity over quality; the case studies in this report often comprised hundreds of online accounts engaged in low-quality, unoriginal deception that was quickly exposed with basic checks. Many of the accounts were newly created, suggesting they are regularly removed by the platforms, and listed locations, languages, and phone numbers that didn't match the persona's claimed location, or gave inconsistent and implausible biographical details. Others impersonated celebrities known to not use social media, or used photos proven by a reverse image search to come from real people's accounts.

Case Studies

Scammers Impersonate U.S. Soldiers in Sprawling 'Stolen Valor' Romance Con

In one cross-platform romance scam, fraudsters masqueraded as U.S. military personnel to target users around the world with hundreds of inauthentic accounts on Facebook, Instagram, Threads, TikTok, Pinterest, YouTube, and the discussion forum Quora. The accounts typically impersonated real U.S. military figures, ranging from senior officials to junior servicemen with no official public presence.

The imposter accounts usually purported to be the impersonated serviceman's real social media account, or a new one created after their real account was compromised by "scammers" or "terrorists." On rare occasions, the impersonator implausibly claimed to be the serviceman's identical twin. The accounts posted about day-to-day life in the U.S. military, sharing content in English and Spanish copied from the real person's authentic social media accounts, as well as U.S. military accounts and websites.

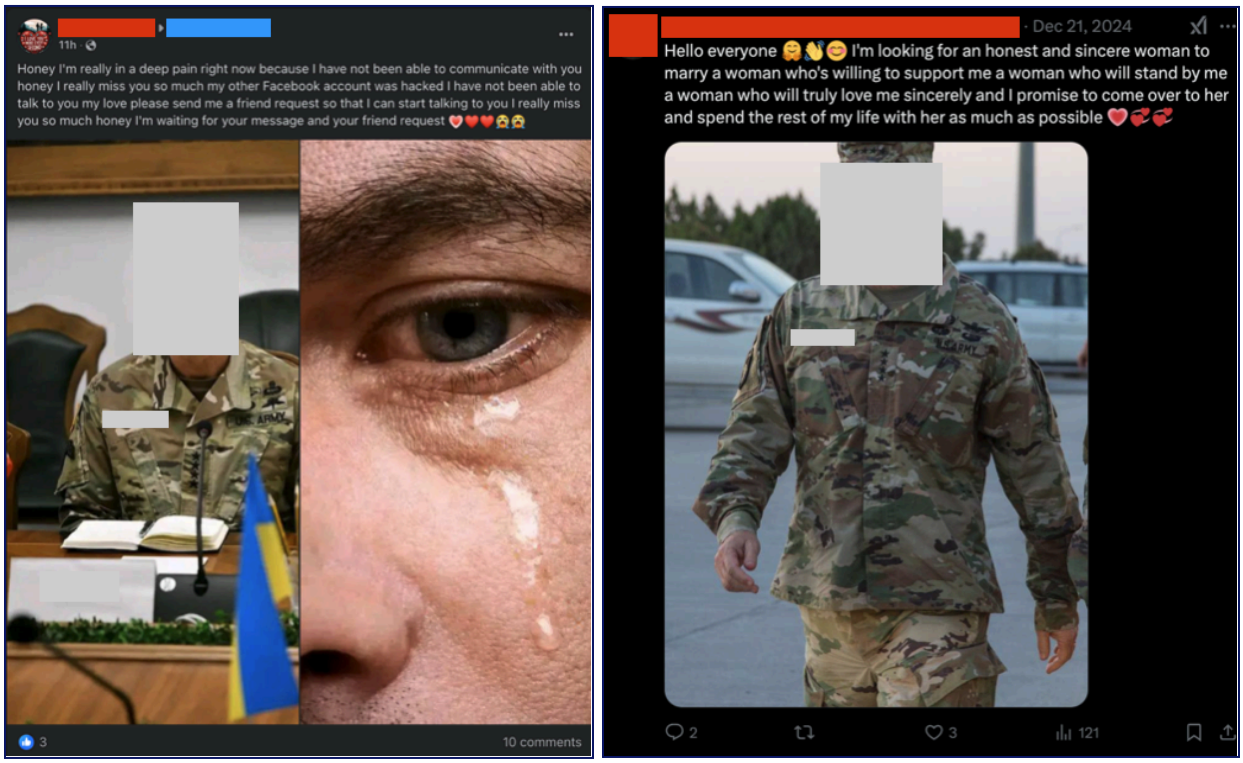
Other fake accounts adopted the personas of fictitious military personnel purportedly based overseas, using fake names and profile pictures of unrelated people. Regardless of whether the impersonated persona was fictional or real, all accounts consistently posted about "feeling lonely" and "looking for love," sometimes sharing sexually suggestive images created using photo editing software.

The fake accounts shared their posts to groups and pages named after the impersonated personnel and also commented on posts by real people talking about the U.S. military or online

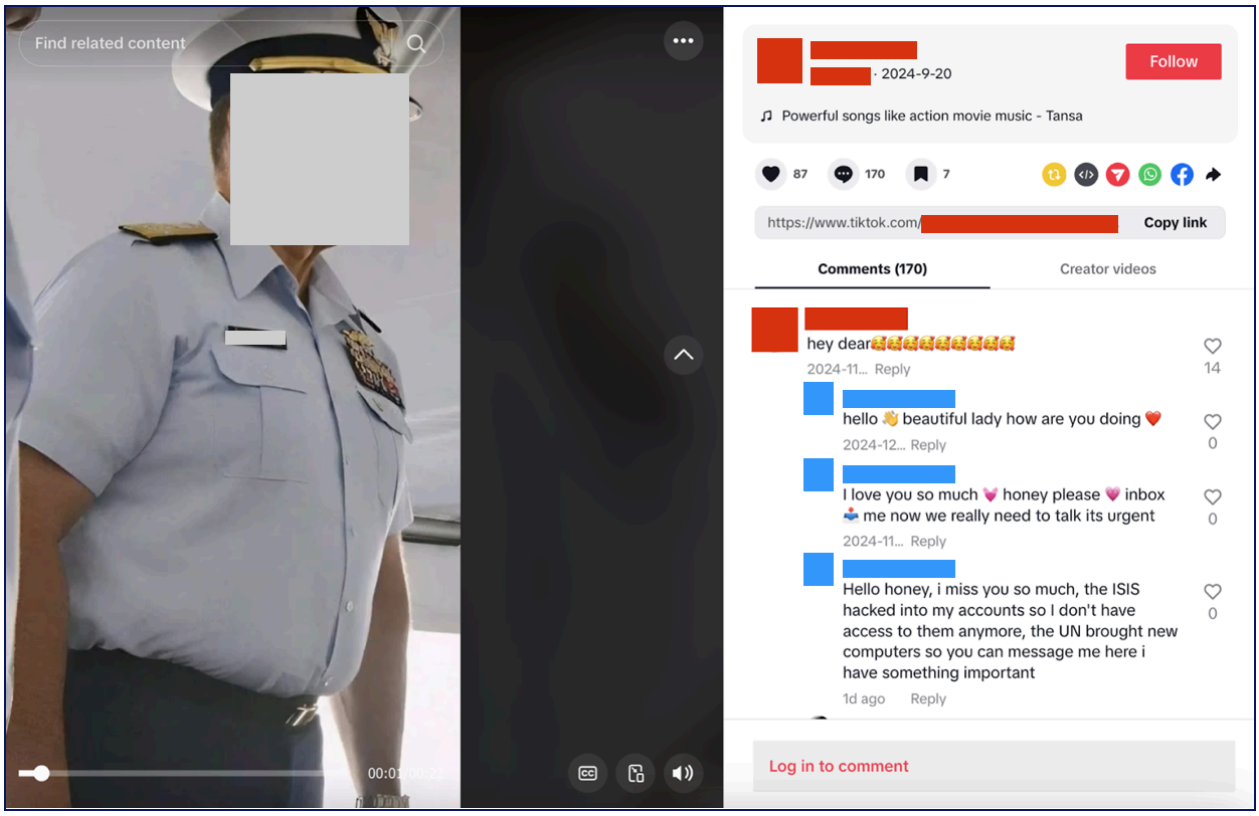
dating and romance. When a real user engaged with their posts, the scammers replied with an invitation to join a private messaging channel, such as WhatsApp, Telegram, Signal, or Facebook Messenger.

According to posts by victims and their families, once in a private conversation, the scammers initiated a romantic relationship with the target. After a short time, the scammers asked them to send money via wire transfer or an online gift card, allegedly to cover the costs of a long-distance phone call or postage for a romantic gift.

The scammers consistently directed targets to contact them via phone numbers with the Nigeria country code; Facebook accounts used in the scam also listed Nigerian "birth city" locations. Some social media users commented on the fake accounts' posts to denounce the activity as a scam, claiming to have spoken with men in Nigeria after initially believing the accounts were authentic.



Inauthentic accounts on Facebook (left) and X (right) impersonating retired U.S. military officials to post about feeling lonely and looking for a romantic relationship. Redactions added by Graphika.



A video posted by an inauthentic TikTok account impersonating a senior U.S. military official attracted a real user's comment, which then received multiple replies from additional inauthentic accounts (blue) impersonating the official and asking the user to contact them privately about an urgent matter. Redactions added by Graphika.

Fake Dating Agencies Charge African Women to Meet 'Rich White Men'

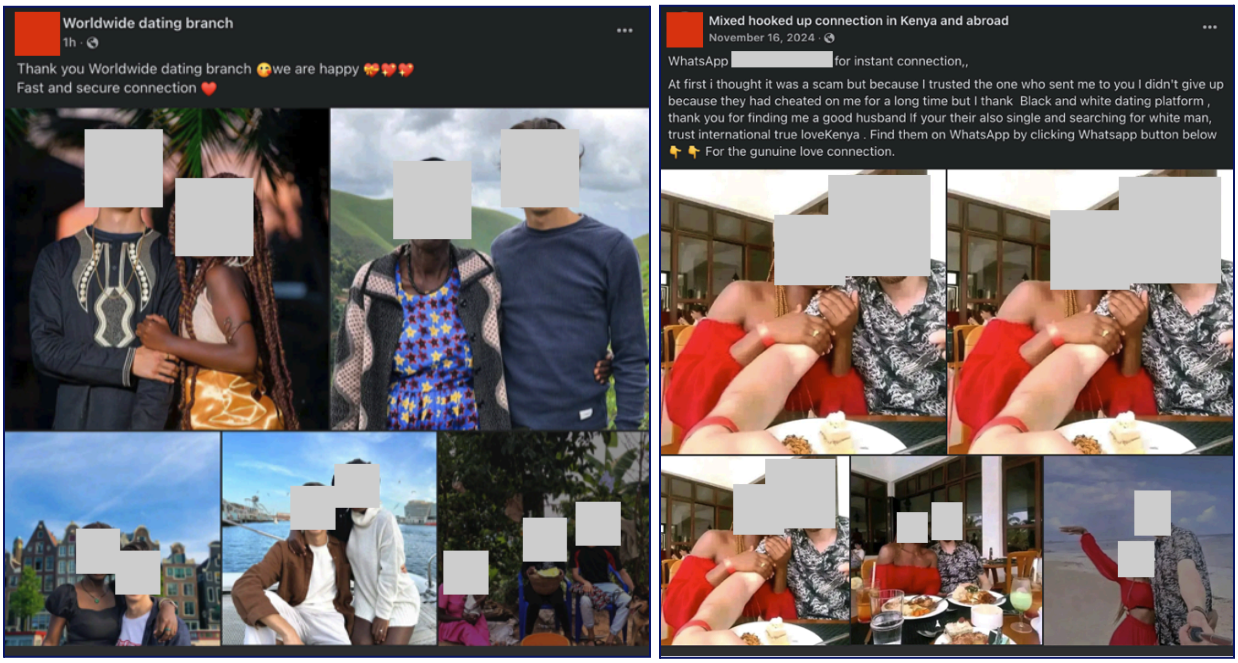
Kenya-linked scammers posed as dating agencies to target African women with fabricated opportunities to meet rich men from Western countries. The network, which operated on Facebook, Instagram, WhatsApp, and Telegram, also included a smaller subset of activity targeting men looking for relationships with "African women."

The scammers created social media accounts claiming to represent dating agencies specialized in interracial relationships, named "Worldwide dating platform," "White Rich men dating platform," or "Rich white men looking for African ladies," for example. The accounts listed contact details in Kenya, and Facebook pages in the network also listed Kenya as their administrator locations.

The "dating agencies" then posted fake "lonely singles" promotions using pictures of real people taken from authentic social media accounts, alongside fictitious biographies that included name, age, occupation, religion, hobbies, and relationship status. The men were usually described as bachelors based in or traveling to Africa and looking for love, and they sometimes promised relocation to a Western country for a future partner. Often, the scammers used the same photo multiple times for different biographies. The fake agencies also shared wedding photos of white men and black women – and childbirth announcements – claiming these were the result of their dating services.

For more information on how to contact the men in the posts, users were told to join a Telegram channel or WhatsApp group registered to a number with a Kenya country code. According to posts by victims on Facebook, Reddit, and other social media platforms, the fake dating agencies then charged users a fee to receive the fictitious man's fake contact details.

Facebook pages claiming to represent dating agencies but using repurposed photos of a Venezuelan celebrity alongside a fake biography. The posts claim the man is looking for a relationship with an African woman. Redactions added by Graphika.



The fake agencies shared photos of white men and black women on Facebook, claiming these relationships were the result of their dating services. Redactions added by Graphika.

Counterfeit Celebrities Target Users With Calls for Love and Gifts

Multiple networks of inauthentic social media accounts impersonated celebrities to lure people from the U.S., United Arab Emirates, Japan, and other countries into fake romantic relationships. This activity comprised hundreds of accounts on platforms including Facebook, Instagram, YouTube, TikTok, and X, as well as private messenger apps and websites.

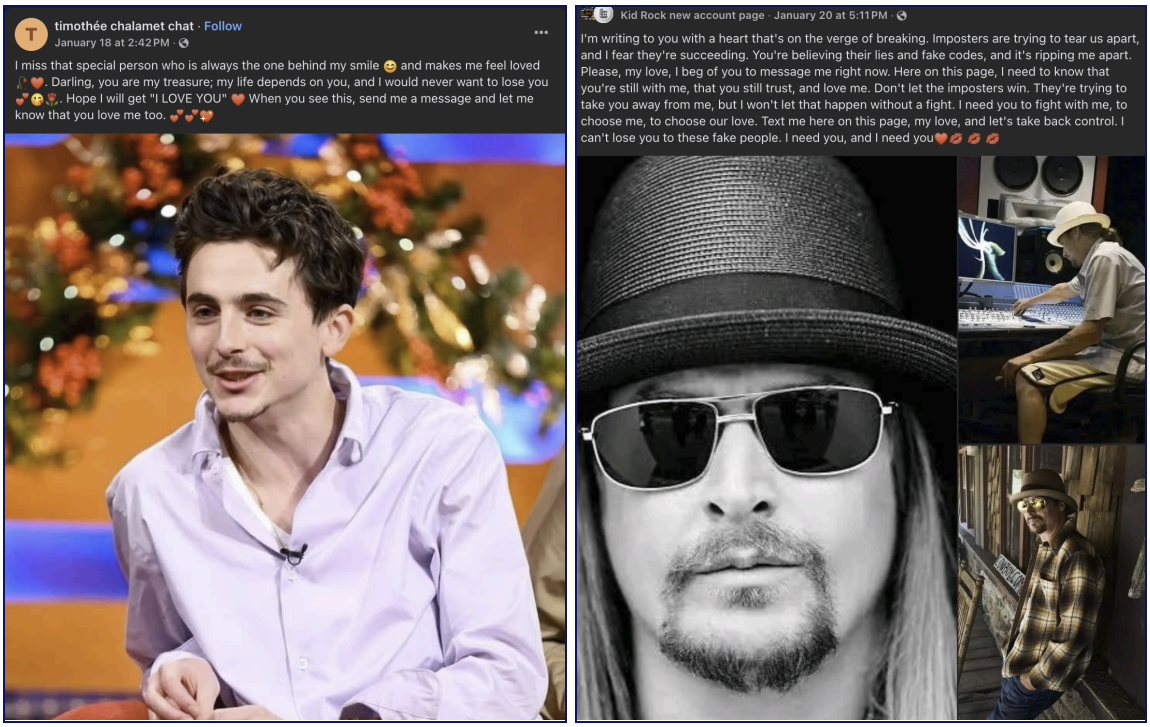
The scammers behaved consistently across all the networks, first creating inauthentic accounts and pages impersonating a celebrity – often someone appropriate for the target audience – or, occasionally, a celebrity's manager and family members. We found accounts targeting users in Japan by impersonating a Japanese musician, for instance, and accounts targeting U.S. users with the persona of an American film star. The accounts typically claimed to be the celebrity's "official" or "personal" social media presence intended only to communicate with their most dedicated fans.

With the inauthentic accounts and pages set up, the "celebrity" then posted content about romance and "looking for love." Common themes included claims of: seeking new love after ending a relationship, feeling too old and ugly to be loved, and being in love with the user(s) and vulnerable to heartbreak if they don't reply. The posts usually included videos and photos of the celebrity, typically sourced from online media reports but sometimes edited to show them in romantic poses and settings.

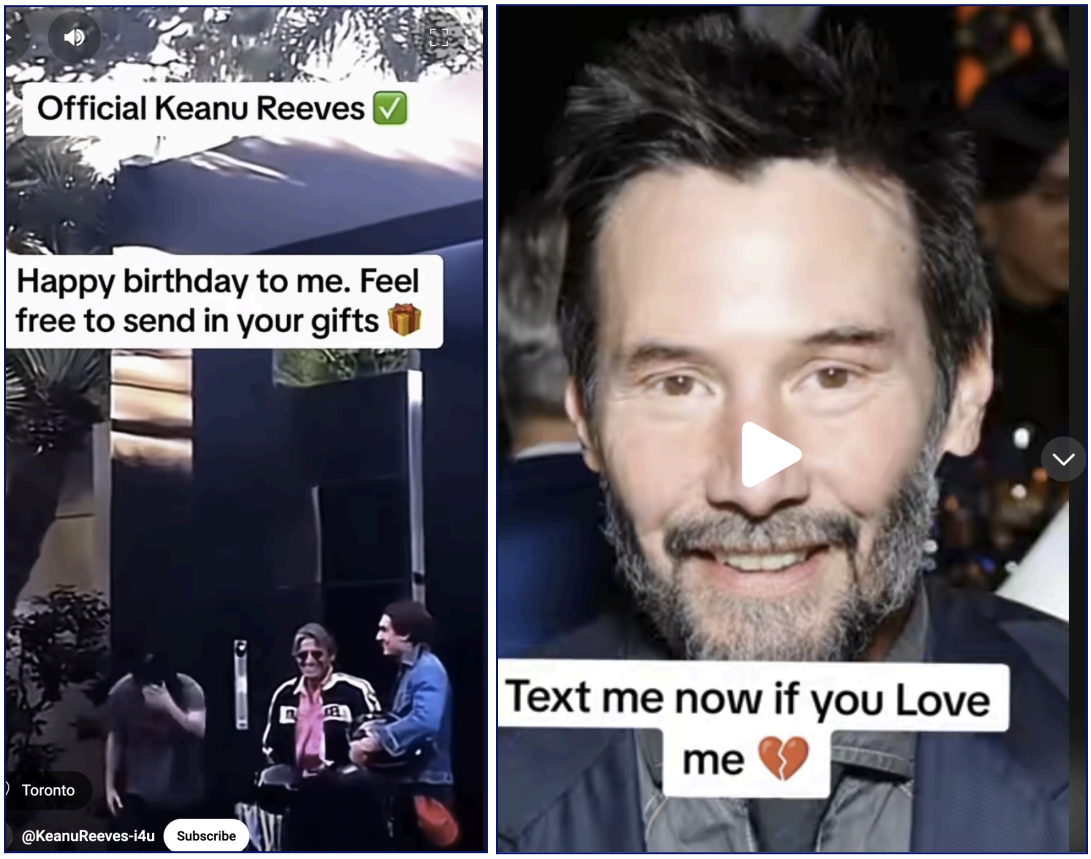
The inauthentic accounts shared the content in "fan groups" for the impersonated celebrity, some of which were very likely operated by the scammers, and in comments on posts by real users talking about the celebrity. When a real user engaged with the content, the scammers asked them to contact the celebrity privately via messaging apps, such as WhatsApp, Signal, or Telegram. In recent weeks, the fake accounts increasingly directed targets to use an encrypted and anonymous messaging service called Zangi, possibly in response to disruption actions by other platforms.

According to posts by victims and their families on Reddit and other discussion forums, once the scammers established direct contact with a target, they asked them to send money via wire transfer, cryptocurrency exchange, or gift cards. The funds were purportedly to help the celebrity purchase romantic gifts or escape financial difficulties. Sometimes the scammers also charged their targets to join "exclusive" paid-access-only fan clubs.

The multiple networks of accounts were very likely operated by actors in different countries who sometimes competed for users' attention and denounced each others' accounts as "fake" and "scammers." Some inauthentic accounts, for instance, consistently encouraged targets to contact them by phone using numbers that feature the Nigeria country code; others were linked to the account of a likely scammer in Bangladesh, who seemingly posted on fake celebrity fan pages using their real account.



Facebook accounts impersonating the actor Timothée Chalamet (left) and musician Kid Rock (right), encouraging users who love them to contact them via private messaging services, such as Zangi.



Scammers impersonating actor Keanu Reeves posted videos to YouTube (left) and TikTok (right), asking users to send gifts and contact him (them) via private message.

Estimative Language Legend

Assessments of Likelihood

Graphika uses the following vocabulary to indicate the likelihood of a hypothesis proving correct. If we are unable to assess likelihood due to limited or non-existent information, we may use terms such as "suggest."

Almost No Chance	Very Unlikely	Unlikely	Real Chance	Likely	Very Likely	Almost Certain(ly)
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

Confidence Levels: Indicators of Sourcing and Corroboration

Graphika uses confidence levels to indicate the quality of information, sources, and corroboration underpinning our assessments.

Low Confidence	Medium Confidence	High Confidence
Assessment based on information from a non-trusted source and/or information we have not been able to independently corroborate.	Assessment based on information that we are unable to sufficiently corroborate and/or information open to multiple interpretations.	Assessment based on information from multiple trusted sources that we are able to fully corroborate.

Graphika

About Us

Graphika *is the most trusted provider of actionable open-source intelligence to help organizations stay ahead of emerging online events and make decisions on how to navigate them. Led by prominent innovators and technologists in the field of online discourse analysis, Graphika supports global enterprises and public sector customers across trust & safety, cyber threat intelligence, and strategic communications spanning industries including intelligence, technology, media and entertainment, and global banking. Graphika continually integrates new and emerging technologies into our proprietary intelligence platform and analytic services, empowering our customers with high-precision intelligence and confidence to operate in a complex and continuously evolving information environment.*

For more information or to request a demo, visit our website.