Wall Street's New Favorite Way to Swap Secrets Is Against the Rules

By **Laura J Keller**
March 30, 2017, 6:00 PM CDT
Updated on March 31, 2017, 5:00 AM CDT

- Encrypted messaging apps are raising risk of widespread abuse
- Employees at big banks share gossip, client data and more

Dirty jokes and NSFW <https://www.merriam-webster.com/dictionary/NSFW> GIFs. Snaps of unsuspecting colleagues on the trading floor. Screenshots of confidential client positions.

All that -- and, on occasion, even legally dubious <https://www.bloomberg.com/news/articles/2016-12-21/n-y-pension-pay-to-play-plot-fueled-by-cash-hookers-u-s-says> information -- is increasingly being trafficked over the new private lines of Wall Street: encrypted messaging services like WhatsApp and Signal.

From traders to bankers and money managers, just about everyone in finance is embracing these apps as an easy, and virtually untraceable, way to circumvent compliance, get around the HR police and keep bosses in the dark. And it's happening despite the industry's efforts to crack down on unmonitored communications, according to conversations with employees at more than a dozen of Wall Street's most recognizable firms.

The widespread use of encrypted apps is also raising a deeper concern: It could enable reckless behavior that's all but impossible to police Photographer: Brent Lewin/Bloomberg

Just this week, a former Jefferies Group <https://www.bloomberg.com/quote/JEF:US> banker was fined in the U.K. for sharing confidential data <https://www.bloomberg.com/news/articles/2017-03-30/ex-jefferies-banker-fined-for-sharing-client-data-on-whatsapp> on WhatsApp.

In many ways, the development reflects a cultural shift. At big banks and small shops alike, rowdy trading desks and the boys-will-be-boys ethos are no longer tolerated, at least publicly. But the widespread use of encrypted apps is also raising a deeper concern: It could enable reckless behavior that's all but impossible to police and lead to abuses like the chat-room scandals involving Libor manipulation and currency rigging.

"You're really able to operate outside of the bank," said William McGovern, a former SEC branch chief and senior lawyer at Morgan Stanley who now works at law firm Kobre & Kim. "We have seen in our investigations that the ground is shifting under everyone, and technology changes are driving a lot of it."

Rules, Regulations

The rules are clear. Financial firms need to keep records of all written business communications, no matter how innocuous, according to the Securities and Exchange Commission and the Financial Industry Regulatory Authority. Asset managers are bound by similar regulations.

Representatives for Wall Street banks, including those at Goldman Sachs Group Inc., Bank of America Corp. and Citigroup Inc., say they have various policies in place to prevent unmonitored communications and unauthorized access to confidential information. They routinely check emails and chats on company devices, restrict personal phones and messaging services on trading floors and require employees to sign agreements prohibiting unmonitored communications for work. In January, Deutsche Bank AG banned <https://www.bloomberg.com/news/articles/2017-01-13/deutsche-bank-is-banning-text-messages-on-company-issued-phones> text messages and apps such as WhatsApp and Apple Inc.'s iMessage on company phones globally to improve compliance standards.

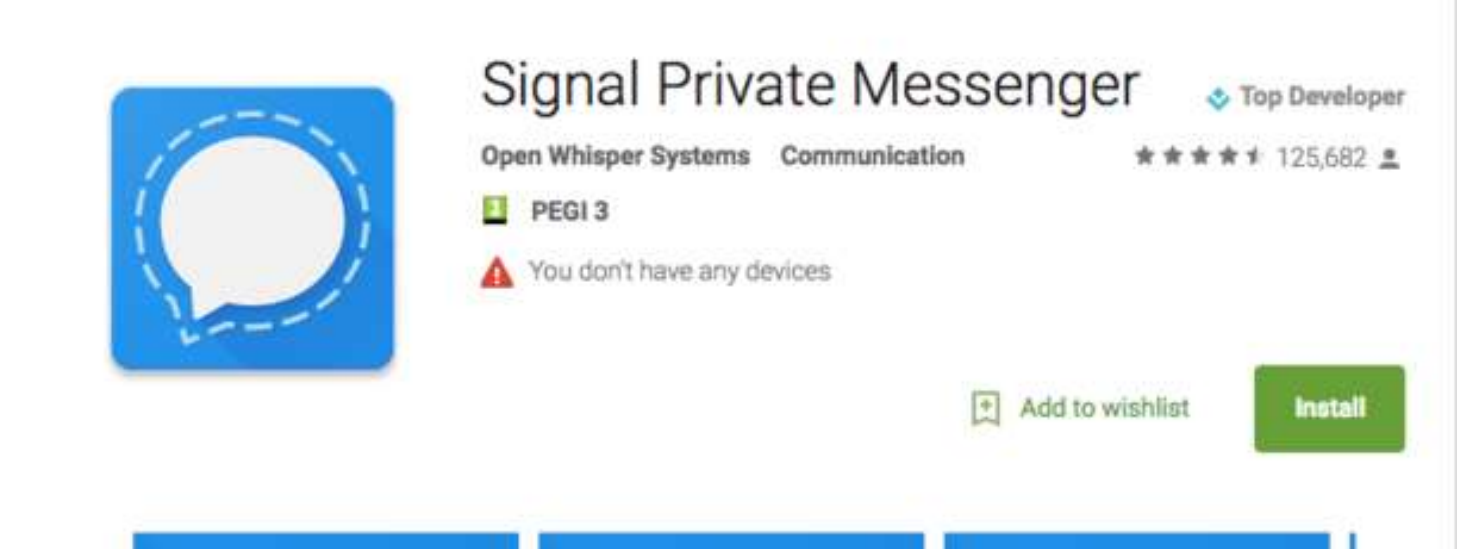
Across finance, the nearly two dozen employees who spoke with Bloomberg say those policies are routinely ignored and the use of personal phones for work is a fact of life. No one would speak on the record for fear of losing their jobs.

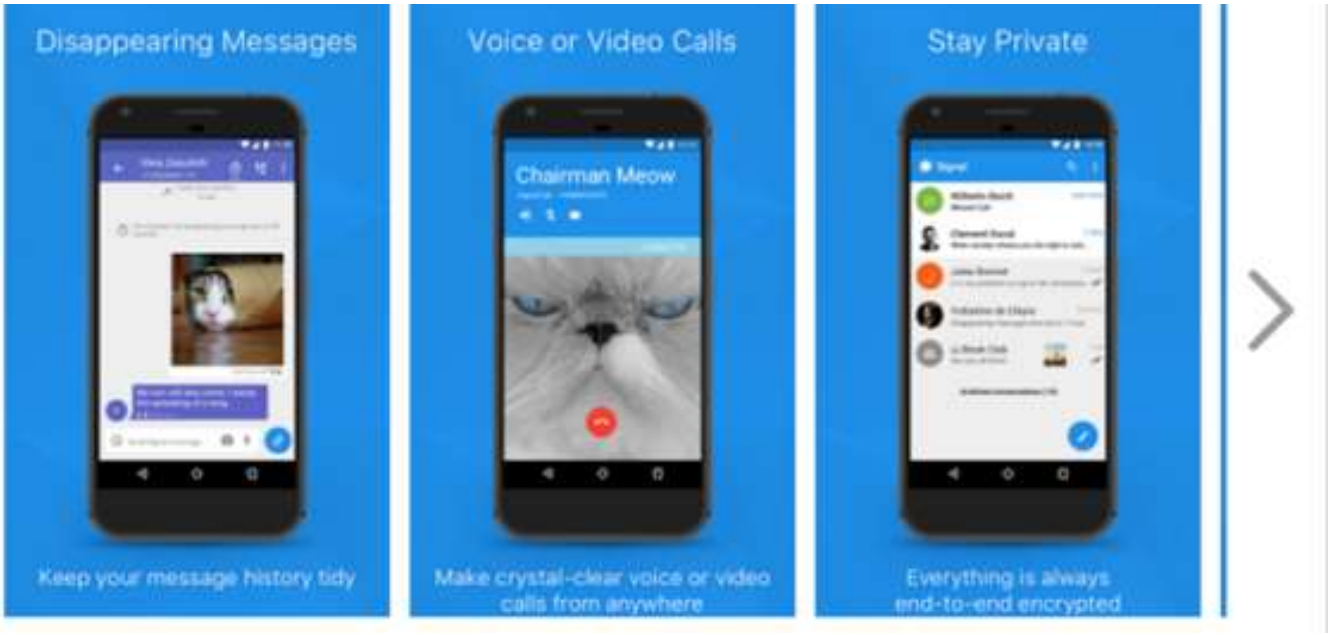
When asked about the widespread use of unauthorized apps, SEC spokeswoman Judith Burns declined to comment.

Big Brother

A big reason more and more Wall Street types have turned to messaging apps is because they are tired of having every written word -- work-related or not -- ingested into vast, Big Brother-like databases and scrutinized for tone and taste in ways that strike many as overbearing. They've learned even the slightest misinterpretation can land them in hot water -- not only with compliance, but with prosecutors on the lookout for financial crimes.

Some clients also prefer those apps to communicate. Ignoring those messages would be bad for business (not to mention how awkward it can be to try and steer conversations back onto monitored systems). Many clients are friends, and vice versa.





Signal is recommended by the likes of Edward Snowden and others worried about government surveillance.

Financial firms have long grappled with new technologies -- think email, chat rooms or instant messaging software like BlackBerry's "BBM" -- and how to balance the privacy of their employees with the need to comply with securities laws. (Bloomberg's message and IB chat services enable firms to set up alerts and restrictions to help enforce compliance.) But in this perennial cat-and-mouse game, it's gotten harder for compliance to keep up.

Popular texting apps, like iMessage, already route conversations around most systems that financial firms use to monitor emails and chats. The proliferation of "end-to-end" encryption services, which can automatically delete messages as soon as they are read, like Mark Cuban's Dust, Confide and Signal (which is recommended by the likes of Edward Snowden and others worried about government surveillance), makes things even harder. Foreign-language apps like China's WeChat pose an added language problem for compliance monitors.

'Always Behind'

"They're always behind," said Jack Rader, a managing director at ACA Compliance Group, which sets up monitoring systems for financial services companies to flag potential regulatory problems. "It's almost impossible for a compliance department within buyside or sellside firms to stay ahead of communications technology that is available for employees."

How encrypted messaging is used varies widely on Wall Street.

At the big banks, employees will often use such apps to share gossip, tell clients during morning sales meetings what they're looking to buy and sell (often within sight of their bosses) or even boast about a particularly profitable trade, the people said. A "don't ask, don't tell" mindset prevails.

After betting big on Brexit, junk-bond traders at one of Wall Street's largest banks crowed about plans for a blowout celebration in a large WhatsApp chat group that included friends from rival firms.

Others say the apps are crucial because they're faster and more convenient than the monitored software their own firms provide.

Sensitive Matters

Several employees at one multibillion-dollar hedge fund set up a WhatsApp group chat to regularly exchange market intelligence with one another, according to a person with direct knowledge of the matter. It's particularly useful if there is a big market move and for money managers traveling to far-flung places who need to be reachable at a moment's notice.

For more sensitive matters, they turn to Signal. The app can be set to delete messages -- from both the sender and receiver -- in as little as five seconds.

Occasionally, the use of personal phones has enabled conduct that would be construed as legally problematic, compliance experts say. At least one investment bank has debt salesmen who routinely send screenshots of chats showing one hedge fund's positions to another client to win more orders, a person with direct knowledge of the matter said.

"If you look the other way on this, it's only going to get worse," said Warren Small, who teaches a program at Middlebury Institute of International Studies for students seeking careers investigating financial crimes, including with the FBI and the Department of Justice. "With financial transactions, temptations and the rewards are just too great."

WhatsApp Boasting

On Thursday, U.K. regulators said they fined Christopher Niehaus, who worked at Jefferies, about $46,000 for sharing confidential client information via WhatsApp while boasting to a personal acquaintance and a friend. The messages came to light after an unrelated complaint led him to voluntarily hand over his phone to Jefferies, a person with knowledge of the situation said. (Jefferies spokesman Richard Khaleel and Niehaus's attorney declined to comment.)

While the authorities said none of the parties in the Jefferies incident traded on the information, it's not hard to see how things could get worse.

In December, Navnoor Kang, a money manager responsible for $50 billion of New York state's pension fund investments, was indicted for accepting at least $180,000 of bribes from two bond salesmen, including a $17,400 watch, prostitutes and cocaine, in return for business that generated millions in commissions. According to the indictment, Kang and one of the salesmen, Gregg Schonhorn, used WhatsApp "in an effort to keep their communications from being monitored by law enforcement."

Mark Geragos, an attorney for Kang, who pleaded not guilty in January, said in an email that the WhatsApp messages were "benign." Spokesmen for FTN Financial, Schonhorn's former firm, and the U.S. Attorney's office, declined to comment. Schonhorn, who pleaded guilty and is cooperating with the government, didn't respond to a request for comment.

Telltale Signs

To some Wall Street types, the big surprise wasn't just the alleged crime, but that they didn't delete the incriminating WhatsApp messages. If they had, compliance experts say authorities would have less to go on because WhatsApp itself doesn't store users' encrypted messages.

Plus, for the most sensitive conversations, employees say they still prefer calling on mobile phones they know aren't monitored, even though there's a remote possibility those records could be subpoenaed. Investment banks regularly monitor only certain trading-floor lines, and at least until 2018, financial firms generally aren't required to record employees' calls.

Regardless, firms are getting better at spotting the telltale signs when an employee wants to go rogue, Rader says. Because so many traders and salesmen rely on persistent chats to talk with clients, banks have taken a page from prosecutors and implemented software to immediately flag phrases like "check your phone," "sent you a text," "take this offline" or "call my cell." Some are set up to find the names of specific messaging programs.

While programs designed to detect unwanted behavior will keep improving, technology can only go so far in keeping Wall Street firms on the right side of the law. When Rader talks to them about compliance, he sometimes encounters pushback from the heads of sales and trading desks, especially because profits are at stake. That raises a whole host of thorny questions, according to Erik Gordon, a professor at the University of Michigan's Ross School of Business.

"Are the firms really doing what's reasonable in trying to stop this?" he mused. "Or are they sort of wink-winking?"

— With assistance by Suzi Ring, and Steven Arons