acin

Risk Intelligence Report

Unauthorised communications become a $2 billion problem for banks

How banks can mitigate fines for e-comms misuse

Despite high levels of fines for record keeping failures, banks are failing to keep tabs on the use of unauthorised communications channels.

As hybrid working has become more common in the wake of the pandemic, the risk of bank employees using unauthorised communication channels such as social media platforms and messaging apps has proliferated.

While Acin flagged WhatsApp and other unmonitored communication-channel use as an emerging risk last year, banks have failed to take action fast enough. Since December 2021, regulators have imposed more than $2 billion in penalties for banks failing to keep records of communications made on personal devices. Even amid that heightened regulatory scrutiny, only 15% of financial institutions currently monitor WhatsApp, according to a SteelEye survey[1].

1 | https://www.steel-eye.com/white-papers-and-e-books/annual-compliance-health-check-report

Part 1:

No longer an emerging risk

Concerns about unauthorised communication use stretches back well before the pandemic. Scrutiny has intensified as the growth in hybrid working increases the risk of bank employees using messaging apps such as WhatsApp, Slack, Signal and others to communicate with clients and colleagues on work-related matters. The Securities and Exchange Commission's (SEC) & Commodity Futures Trading Commission's (CFTC) investigations have shown the problem is pervasive—it is not just traders or junior staff communicating in this way; supervisors and other senior managers are also using unmonitored non-work applications to send work-related messages.

Why have we not learnt from previous operational risk events?

2006

The SEC charged Morgan Stanley $15 million and ordered them to adopt and implement procedures for the preservation and production of email communications.

2012

The Libor Scandal highlighted the use of instant messaging channels used for market manipulation.

2017

The first case of regulators cracking down on social media - The UK Financial Conduct Authority (FCA) warned about the risks of using WhatsApp. A Jefferies managing director was fined £37,198 by the FCA, for sharing clients' confidential information and boasting about deals over WhatsApp.

December 2018

SEC guidance reminding companies of their responsibility to monitor electronic messaging including instant messaging apps, personal emails and texting.

August 2019

KPMG dismissed its head of financial services consulting in the UK following a probe linked to messages sent using the popular messaging service WhatsApp.

July 2020

FMSB publishes spotlight review examining remote working risks.

April 2020

JPMorgan suspended a senior credit trader for using a WhatsApp group to communicate with colleagues, underscoring the growing worry over the use of unauthorised communication channels.

October 2020

Two top Morgan Stanley commodities traders lose jobs over the use of WhatsApp as Wall Street continues clamp down on communications channels it cannot monitor.

November 2020

Credit Suisse launches WhatsApp rival for staff as banks grapple with text tracking.

October 2021

SEC opens their enquiry into how Wall Street are surveying employees communication.

December 2021

JPM is fined $200m by the SEC and the CFTC marking the start of a wave of fines which reach $2bn in 2022.

February 2022

The CFTC investigated HSBC for the use of non-approved messaging platforms for business communications.

February 2022

The SEC probed Citigroup over employees using communication channels not approved by the bank and investigated its record-keeping compliance.

May 2022

The SEC forced Wall Street banks to embark on a systematic search through more than 100 personal mobile phones carried by top traders and dealmakers in the largest-ever probe into clandestine messaging on platforms such as WhatsApp.

June 2022

Bankers at Deutsche Bank are asked to install an app that tracks communications on their phones as regulators crack down on messaging between bankers and clients on unauthorised platforms.

June 2022

Credit Suisse Group AG's former global head of equity capital markets syndicate was removed from his position after being found to have used unauthorised messaging services when communicating with clients.

July 2022

The world's largest banks including Morgan Stanley, Bank of America, Goldman Sachs, Citigroup, Deutsche Bank, UBS and Barclays said they have provisioned around $200 million each for potential fines related to SEC and CFTC probes into unauthorised communications use.

August 2022

Jefferies is fined $80 million in Wall Street texting investigation.

September 2022

SEC and CFTC fine the worlds largest investment banks a total of $2.01bn, making them the biggest penalties ever against banks operating in the US for record-keeping failures.

September 2022

Asset managers are also now on alert.
DWS has already set aside $12 million to cover potential US fines related to its employees' use of unapproved devices and record-keeping failings.
Other investment firms including Amundi, AXA Investment Management, BNP Asset Management and JPMorgan Asset Management have deployed tools to ensure communications between staff and clients are compliant.

Part 2:

Increasing risk factors

The Financial Markets Standards Board (FMSB) published 9 key risks of remote working

- Control limitations
- Execution risks
- Governance
- Heightened cyber risk
- Sales lifecycle
- Sharing confidential information
- Staff treatment and productivity
- Third party risk
- Threats to market effectiveness

Acin's Risk Intelligence team has identified four groupings of controls based on the nine FMSB risks[2] that are relevant to heightened e-communications risk and which risk managers should be focused on.

The 4 categories that Acin's analysis focuses on are

- Surveillance
- Training and supervision
- Employee monitoring
- Business continuity planning

These 4 categories are based on a review of the controls within the circled FMSB risk categories shown above and Acin's own analysis of required controls.

Clients should look at the frequency of their controls vs. the Acin Network:

Acin's analysis included an analysis of 28 unique controls that appear 156 times across clients and inventories across the 4 categories identified. The analysis highlights that banks should carry out a review of their controls and must improve control design to manage the risk of unauthorised communications more effectively.

3% of controls are not documented
across the 4 categories of controls. Given regulatory scrutiny, not being able to evidence the documentation of these controls in a risk and control inventory makes it impossible to convince a regulator that these controls do exist and are monitored.

20% of client controls are poorly documented
These controls did not have a control type documented. How are assurance functions able to monitor and, or test controls if they do not know whether a control is preventative or detective?

18%
of controls operated less frequently than peers

50%
in line with Acin or more frequent

31%
have no frequency attribute

2 | https://fmsb.com/fmsb-publishes-spotlight-review-on-examining-remote-working-risks-in-ficc-markets/

Part 3:

Fixing the gaps

Banks are missing a range of controls that can prevent and detect e-communications risk. Do you know where your gaps are?

- Acin's network data reveals that within these four groupings, there are 28 unique controls that appear in our data sets across 156 control and inventory instances. On average of the control instances analysed 24% of these are preliminary missing across our clients for the controls in scope for this analysis.
- Of these 24% of controls noted as preliminary missing on initial analysis, after discussion with our clients on average we find that 34% are categorized as missing and 19% remain under investigation as preliminary missing.

156 control and inventory instances, where 24% of these are preliminary missing

Being out of the line of sight makes it difficult for managers and compliance teams to monitor behaviour[3]. Four categories of controls banks need to review to manage the risk of unauthorised communications use:

Surveillance

- **Problem:** Employees may deliberately circumvent controls and surveillance (such as recorded phone lines) to commit fraud or other types of misconduct
- **Fix:** Ensure monitoring apps are installed on personal devices to reduce the risk of unauthorised communication channels use

Training and Supervision

- **Problem:** Poor people management can result in employees being unaware of the rules around unauthorised communications use
- **Fix:** Make sure employees understand what channels they can use and how to communicate with clients and colleagues in an authorised way

Employee Monitoring

- **Problem:** Surveillance controls are insufficient on their own
- **Fix:** Consider implementing macro controls that can provide early warning signs of rogue employee behaviour

Business Continuity Planning

- **Problem:** Employees are tempted to switch to unauthorised channels to get work done during periods of market volatility or if it is not possible to access authorised channels
- **Fix:** Provide access to and clear procedures for using recorded phone lines when employees are working remotely

3 | https://www.fca.org.uk/firms/remote-hybrid-working-expectations

Part 4:

Mitigating the risk

Here are a few examples of controls banks should adopt to better detect and prevent the use of unauthorised communications channels:

Off premises trade surveillance review	To ensure employees are being adequately monitored when working remotely
Joiners, Leavers, Movers Review	To monitor for talent risk and to ensure the right people with the right behaviours are being hired
Out-of-Hours Monitoring	To prevent unauthorised communications use when employees are working on transactions outside of normal office hours
Business continuity plan testing	To prevent the risk of business disruption due to a failure to recover from internal or external shock

Acin's Risk Scenario

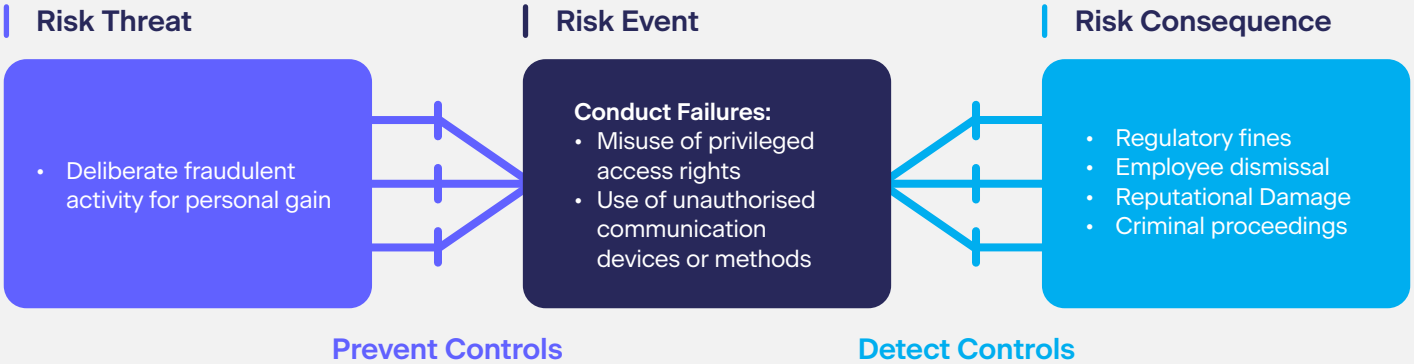
Its important to note that the SEC and CFTC investigations went back to 2018 – then it may have been easier to detect with a model of supervisors having their employees in their line of sight now it is much harder to manage let alone prevent. So firms need to look at behaviours and threats that may lead to the use of unauthorised comms.

Acin's Risk Scenarios enable firms to easily conduct a read across with risks and controls already mapped. We use the bow tie method to bring current and emerging themes to life so that firms can manage risk in a practical manner.

Example

Risk Statement: Use of sensitive information for personal gain leads to employee dismissal

Risk Narrative: A compliance officer searched the compliance system and retrieved information relating to proposed takeovers and mergers. This information was then disclosed to a colleague who traded in the shares of related companies for personal gain. Both individuals sought to conceal their criminal activity over the course of a year by using pay as you go mobile phones and swapping sim cards to discuss their planned activities.



Detection Method: The event was detected through a review of system access rights by audit and subsequent review of computer records, trading data, and unauthorised communication channels by the regulator.

Acin's platform digitises operational risk, provides access to network data and ensures risks and controls are complete, effective and in line with best practice.

Acin's analysis covers front to back controls and can easily find where firms can direct their attention.

On average approx 10%

front office controls are found to be non controls or unclear

Approx 3%

of front office controls are confirmed as missing or not documented

About Acin

Founded in 2018, Acin has built the defining data network for operational risk control, for leading financial institutions.

Acin's award-winning Risk Control Diagnostics platform digitizes and assures operational risk controls in a connected data network across the financial services industry. Backed by Fitch, and trusted by JP Morgan, Credit Suisse, Standard Chartered and other pioneers, Acin assures operational risk controls are complete, efficient and calibrated to the market.

For more information

70 Gracechurch Street,
London EC3V 0HR.

+44 (0)20 3728 8585

connect@acin.com

acin.com

Follow us on LinkedIn

Twitter @AcinTweets