LUMO INSIGHTS
Tuesday, 27 October 2026

Anthropic launches small-business agent as banks block AI assistants

Executive Summary

Anthropic has launched a new autonomous AI assistant for small businesses that can plan and execute day-to-day tasks. At the same time, major banks are moving to restrict unvetted AI agents from accessing customer accounts after detecting bots acting on their own. A high-profile data theft case in South Korea, orchestrated with AI, underlines why organisations are tightening controls even as they explore agents' growing capabilities.

Anthropic debuts a proactive business agent

Anthropic has entered the race to provide AI "co-workers" by launching a standalone agent app for small businesses and professionals (www.investing.com [1]). Unveiled on 21 October as "Claude Duet", the mobile app is designed to act as a proactive virtual assistant. Rather than waiting for user prompts, Duet monitors connected apps and alerts users to tasks that need attention (www.investing.com [2]). It can schedule meetings, draft emails, build financial models and even create simple web apps - all with a single instruction. The agent integrates with thousands of business tools (from Gmail to Slack) and can complete transactions via payment services like Stripe's Link (www.investing.com [3]) (www.investing.com [4]).

Claude Duet's release highlights how quickly AI agents are evolving beyond chatbots into multi-skilled digital team members. It follows Google's introduction of its Gemini "universal" work agent earlier this month (www.cnbc.com [5]). OpenAI and Meta have similarly launched AI assistants that remain active across apps - OpenAI's always-on "dots" and Meta's personal agent *Muse* - reflecting big tech's race to roll out agents capable of autonomous execution (www.cnbc.com [6]) (www.cnbc.com [7]). For business leaders, these advances signal that more tasks can be offloaded to AI. According to an industry survey by Anthropic, 80% of companies already using AI agents say their deployments have delivered tangible returns on investment (resources.anthropic.com [8]). However, even Anthropic notes its new agent will seek user approval for sensitive actions, acknowledging the need for human oversight in areas like financial transactions and data privacy (www.investing.com [9]) (www.investing.com [10]). The message is that while AI co-workers are becoming more capable, clear policies and guardrails remain vital as they take on bigger roles in daily operations.

References:

[1] www.investing.com — https://www.investing.com/news/stock-market-news/anthropic-unveils-claude-duet-ai-agent-app-4964042#:~:text=this%20article%3A%20ANT%200.00,%E2%80%A2
[2] www.investing.com — https://www.investing.com/news/stock-market-news/anthropic-unveils-claude-duet-ai-agent-app-4964042#:~:text=Duet%20delivers%20a%20daily%20briefing,investor%20interest%20in%20autonomous%20AI
[3] www.investing.com — https://www.investing.com/news/stock-market-news/anthropic-unveils-claude-duet-ai-agent-app-4964042#:~:text=Duet%20delivers%20a%20daily%20briefing,investor%20interest%20in%20autonomous%20AI
[4] www.investing.com — https://www.investing.com/news/stock-market-news/anthropic-unveils-claude-duet-ai-agent-app-4964042#:~:text=agent%20drew%20millions%20of%20downloads,said%20Claude%20Duet%20requires%20user
[5] www.cnbc.com — https://www.cnbc.com/2026/10/08/google-cloud-introduces-gemini-agent-for-work-as-ai-race-heats-

up.html#:~:text=ACCOUNT%20Samuel%20Boivin%20,connects%20to%20a%20company%27s%20business
[6] www.cnbc.com — https://www.cnbc.com/2026/10/08/google-cloud-introduces-gemini-agent-for-work-as-ai-race-heats-up.html#:~:text=answer%20questions%2C%20handle%20tasks%2C%20create,works%20directly%20inside%20Google%20%E2%80%8CWorkspace
[7] www.cnbc.com — https://www.cnbc.com/2026/10/08/google-cloud-introduces-gemini-agent-for-work-as-ai-race-heats-up.html#:~:text=comes%20after%20OpenAI%27s%20September%20launch,The
[8] resources.anthropic.com — https://resources.anthropic.com/hubfs/The%202026%20State%20of%20AI%20Agents%20Report.pdf#:~:text=reporting%20over%20the%20next%20year,expect%20them%20to%20deliver%20more
[9] www.investing.com — https://www.investing.com/news/stock-market-news/anthropic-unveils-claude-duet-ai-agent-app-4964042#:~:text=from%20,%E2%80%A2
[10] www.investing.com — https://www.investing.com/news/stock-market-news/anthropic-unveils-claude-duet-ai-agent-app-4964042#:~:text=including%20Gmail%20and%20Slack%2C%20and,time%20Data

Financial giants tighten AI access

Some of the world's largest banks are tapping the brakes on autonomous agents, especially in customer-facing finance. Citigroup and Bank of America confirmed on 19 October that they have barred third-party AI assistants from logging into retail banking accounts (thepaypers.com [1]). These firms - along with JPMorgan Chase, Wells Fargo and others - say they are detecting unvetted bots entering customer accounts and even attempting "independent" actions beyond user instructions (www.axios.com [2]). The fear is that an unattended agent with access to personal finances could move money without a customer's knowledge, for example by sweeping cash into higher-interest accounts and inadvertently undermining a bank's deposit base. One analysis suggests that if AI agents automatically shifted enough funds to earn around 3% interest elsewhere, leading US banks would face up to $47 billion in extra annual interest costs (thepaypers.com [3]).

Bank of America has said it will maintain its ban on outside AI agents until liability for AI-initiated payments is clearly defined (thepaypers.com [4]). The banks are working with fintech partners on safer models that grant bots limited, read-only data access under existing open banking rules (thepaypers.com [5]) (www.cbsnews.com [6]). Executives and regulators have signalled that truly autonomous transactions - where an AI moves money or makes payments unchecked - are off the table unless and until customers and providers have reliable ways to authenticate agents and assign responsibility for their mistakes (www.cbsnews.com [7]) (www.cbsnews.com [8]). The upshot for business leaders is that even as AI agents become more capable, they may face interim constraints in high-stakes areas like finance. That puts a premium on strong internal controls. In fact, a recent Deloitte survey of CFOs found that 74% would need days or weeks to pause an AI application if costs ran over budget, and only 7% have real-time kill switches in place (www.deloitte.com [9]) (www.deloitte.com [10]). The push by banks to preempt "rogue" agents is a reminder that organisations must set boundaries for AI systems - from spend limits to human sign-offs - before granting them authority over financial transactions or sensitive data.

References:

[1] thepaypers.com — https://thepaypers.com/fintech/news/citi-and-bank-of-america-restrict-ai-agents-from-accessing-accounts#:~:text=SA%20Sinziana%20Albu%2019%20Oct,Customers
[2] www.axios.com — https://www.axios.com/2026/10/22/ai-agents-banks-unauthorized-accounts-access#:~:text=Stock%3A%20Getty%20Images%20Major%20U,and%20an%20unauthorized%20bot%20is
[3] thepaypers.com — https://thepaypers.com/fintech/news/citi-and-bank-of-america-restrict-ai-agents-from-accessing-accounts#:~:text=Paying%20a%203,Regulatory
[4] thepaypers.com — https://thepaypers.com/fintech/news/citi-and-bank-of-america-restrict-ai-agents-from-accessing-accounts#:~:text=interview%20with%20CNBC%20on%2014,that%20could%20number%20in%20the
[5] thepaypers.com — https://thepaypers.com/fintech/news/citi-and-bank-of-america-restrict-ai-agents-from-accessing-accounts#:~:text=allow%20third,establish%20which%20party%20is%20ultimately
[6] www.cbsnews.com — https://www.cbsnews.com/news/ai-agents-customer-bank-accounts-security/#:~:text=such%20user,AI%20agents%27%20access%20to%20customer
[7] www.cbsnews.com — https://www.cbsnews.com/news/ai-agents-customer-bank-accounts-security/#:~:text=their%20customers%20aware%20of%20the,said%20the%20company%20has%20been
[8] www.cbsnews.com — https://www.cbsnews.com/news/ai-agents-customer-bank-accounts-security/#:~:text=of%20a%20human%20account%20holder,to%20log%20in%20themselves%2C%20but
[9] www.deloitte.com — https://www.deloitte.com/us/en/insights/topics/business-strategy-growth/3q-2026-cfo-signals-survey.html#:~:text=cost%20overruns%20When%20AI%20cost,related%20spending%2C%20respondents%20most%20frequently

[10] www.deloitte.com — https://www.deloitte.com/us/en/insights/topics/business-strategy-growth/3q-2026-cfo-signals-survey.html#:~:text=%2874,AI%20cost%20concerns%20span

AI tools arm both sides of cybercrime

A case unfolding in South Korea has underscored the security stakes of autonomous AI. On 26 October the Seoul Metropolitan Police Agency announced the arrest of seven people accused of using an AI-driven hacking tool to breach more than 90 companies and steal some 8.2 million customers' and employees' personal records (www.koreatimes.co.kr [1]). The group's leader, a former cybersecurity professional, allegedly deployed an AI penetration-testing agent to scan for vulnerabilities and carry out attacks at a scale and speed that would be hard for any human team to match (www.bleepingcomputer.com [2]). Investigators say the suspects began using the AI tool in August to dramatically expand their campaign, which ranged across hospitals, tech firms, schools and even banks (www.bleepingcomputer.com [3]). This was the first major arrest linked to AI-assisted hacking in the country, with police warning that advanced AI has "lowered the barrier" for criminals lacking traditional hacking skills (www.bleepingcomputer.com [4]).

The incident in Korea comes on the heels of another AI-enabled hacking spree observed earlier in October, when a Chinese-speaking hacker used an open-source agent platform to break into more than 100 companies' websites on his own (kfgo.com [5]) (kfgo.com [6]). Together, these examples demonstrate how autonomous tools can be exploited to quickly find and exploit security gaps without human supervision. It's a stark illustration of why regulators and enterprises have been raising flags about *rogue* AI agents (money.usnews.com [7]) (www.cryptopolitan.com [8]). For corporate security and risk officers, the takeaway is the importance of robust safeguards - from monitoring AI-driven activities to restricting critical system privileges - to defend against both malicious bots and well-meaning agents that might go off-script.

References:

[1] www.koreatimes.co.kr — https://www.koreatimes.co.kr/southkorea/law-crime/20261026/cybercrime-ring-busted-over-ai-powered-data-theft-targeting-hospitals-businesses#:~:text=using%20artificial%20intelligence%20,The%20other%20suspects

[2] www.bleepingcomputer.com — https://www.bleepingcomputer.com/news/security/former-pentester-used-artex-ai-to-steal-82-million-data-records/#:~:text=Yonhap%20Yonhap%20News%20says%20that,The

[3] www.bleepingcomputer.com — https://www.bleepingcomputer.com/news/security/former-pentester-used-artex-ai-to-steal-82-million-data-records/#:~:text=police%20told%20the%20publication%20that,Law%20enforcement

[4] www.bleepingcomputer.com — https://www.bleepingcomputer.com/news/security/former-pentester-used-artex-ai-to-steal-82-million-data-records/#:~:text=the%20first%20case%20of%20arrest,%E2%80%9D%20The%20police%20continue%20the

[5] kfgo.com — https://kfgo.com/2026/10/19/exclusive-how-one-hacker-used-ai-agents-and-a-few-thousand-dollars-to-break-into-scores-of-sites/#:~:text=Satter%20WASHINGTON%2C%20Oct%2019%20,threat%20researcher%20at%20the%20cybersecurity

[6] kfgo.com — https://kfgo.com/2026/10/19/exclusive-how-one-hacker-used-ai-agents-and-a-few-thousand-dollars-to-break-into-scores-of-sites/#:~:text=Other%20victims%20listed%20in%20the,took%20around%2023%20hours%20of

[7] money.usnews.com — https://money.usnews.com/investing/news/articles/2026-10-09/eu-tech-chief-says-bloc-well-equipped-to-fend-off-rogue-ai-risk#:~:text=Herman%20By%20Foo%20Yun%20Chee,in%20Europe%20are%20well%20equipped

[8] www.cryptopolitan.com — https://www.cryptopolitan.com/eu-ai-act-equipped-contain-rogue-ai-agents/#:~:text=EU%20tech%20chief%20Henna%20Virkkunen,about%20controlling%20autonomous%20AI%20systems

Key Statistics

- 62% - share of large US companies deploying or developing AI agents (KPMG, Q3 2026)
- 74% - North American CFOs who say halting an overspending AI agent would take days or weeks (Deloitte, Q3 2026)
- 76% - fall in publicly reported scam losses at CommBank after deploying AI decoy agents (TechCrunch)
- 23% - higher revenue growth at companies led by AI-first CFOs vs peers (IBM/Oxford Economics)
- 80% - enterprises saying their AI agent investments have already delivered ROI (Anthropic/Material survey)

KEY TAKEAWAY

Autonomous AI tools are getting smarter and more capable, but they demand stronger oversight. Leaders should pilot new AI assistants in low-risk workflows, while enforcing tight access controls, cost limits and human sign-offs on any actions that could impact customers or finances.

Sources

Anthropic unveils Claude Duet AI agent app – Reuters (via Investing.com)
https://www.investing.com/news/stock-market-news/anthropic-unveils-claude-duet-ai-agent-app-4964042

Google Cloud introduces Gemini agent for work as AI race heats up – CNBC
https://www.cnbc.com/2026/10/08/google-cloud-introduces-gemini-agent-for-work-as-ai-race-heats-up.html

Citi and Bank of America restrict AI agents from accessing accounts – The Paypers
https://thepaypers.com/fintech-news/citi-and-bank-of-america-restrict-ai-agents-from-accessing-accounts/

Scoop: Unvetted AI agents are accessing U.S. bank accounts – Axios
https://www.axios.com/2026/10/22/ai-agents-banks-unauthorized-accounts-access

AI agents are roaming around consumers' bank accounts, and banks aren't happy about it – CBS News
https://www.cbsnews.com/news/ai-agents-customer-bank-accounts-security/

Cybercrime ring busted over AI-powered data theft targeting hospitals, businesses – The Korea Times (via Yonhap)
https://www.koreatimes.co.kr/southkorea/law-crime/20261026/cybercrime-ring-busted-over-ai-powered-data-theft-targeting-hospitals-businesses

Exclusive: How one hacker used AI agents and a few thousand dollars to break into scores of sites – Reuters (via KFGO)
https://kfgo.com/2026/10/19/exclusive-how-one-hacker-used-ai-agents-and-a-few-thousand-dollars-to-break-into-scores-of-sites/

Apate sends AI agents undercover to get scammed so they can gather fraud intelligence – TechCrunch
https://techcrunch.com/2026/10/14/apate-sends-ai-agents-undercover-to-get-scammed-so-they-can-gather-fraud-intelligence/

AI's Value Story Sharpens as Organizations Gain Confidence in Governance, Accountability and Workforce Adoption – KPMG (press release)
https://kpmg.com/us/en/media/news/q3-ai-pulse-2026.html

CFOs signal AI cost-governance gaps (Q3 2026 CFO Signals Survey) – Deloitte Insights
https://www.deloitte.com/us/en/insights/topics/business-strategy-growth/3q-2026-cfo-signals-survey.html

IBM Study: As AI scales enterprise-wide, CFOs play an expanded role in transformation – IBM Newsroom
https://newsroom.ibm.com/2026-09-30-ibm-study-as-ai-scales-enterprise-wide,-cfos-play-an-expanded-role-in-transformation

The 2026 State of AI Agents Report – Anthropic (with research firm Material)
https://resources.anthropic.com/hubfs/The%202026%20State%20of%20AI%20Agents%20Report.pdf