



Sinch AB

Vi identifierade Sinch AB som den ledande möjliggöraren av bluffsamtal och robotsamtal mitt i stigande regulatoriskt tryck

Stockholm: SINCH

Denna version av rapporten är en översättning avsedd för våra svenska läsare och kann innehålla fel. Den ursprungliga rapporten finns tillgänglig på engelska och har företräde över den översatta versionen.

- Sinch AB (STO: SINCH) är ett Sverige-baserat företag som verkar som en leverantör av kommunikationsplattform som tjänst (CPaaS) och som möjliggör för företag att kommunicera med kunder via SMS, rik meddelandehantering (RCS/WhatsApp), röst, video, e-post och verifieringstjänster genom API:er.
- Sinch förvärvade Inteliquent, som vi anser vara en viktig finansiell drivkraft för Sinch. Vår analys avslöjar att Inteliquent är den enskilt största möjliggöraren av bluffsamtal och robotsamtal i västra halvklotet, med verksamheten som står inför regulatorisk granskning.
- Medan investerare verkar till stor del omedvetna om de bluffsamtalsproblem som är relaterade till Inteliquent, är regulatorer runt om i världen det inte. Anti-Robocall Task Force, ledd av justitieministrarna i Indiana, North Carolina och Ohio, fann i december 2025 att Inteliquent är ansvarigt för nästan hälften av alla robotsamtal i USA. Vi ser hur regulatorer stänger in sig på

företaget, vilket vi förväntar oss kommer att avsevärt skada Sinchs ekonomi. Inget av detta har ännu avslöjats för investerare.

- Vi konsulterade experter och fann högkvalitativ forskning som bluffrapporteringsgemenskapen har utfört. Sinch och dess dotterbolag exponerades konsekvent som de värsta aktörerna i branschen och som viktiga möjliggörare av bluffsamtalsindustrin.
- Vår analys av Sinchs dotterbolag ur ett konsumentperspektiv indikerar att de är bland de mest frekvent citerade för att möjliggöra bluffsamtal och robotsamtal. I synnerhet verkar konsumenter mest upprörda över Sinch för bristen på åtgärder mot bedrägliga uppringare.
- Sinchs system innefattar flera lager mellan sig självt och de bedrägliga användarna av dess tjänst. Detta förändrar inte det faktum att det ligger inom Sinchs makt och ansvar att stoppa missbruket.
- Vi anser att Sinchs efterlevnadsteam är otillräckligt både vad gäller omfattning och effektivitet med tanke på volymen av bluffsamtal och robotsamtal som dess plattform kan möjliggöra, särskilt i förhållande till jämförbara aktörer. Detta stämmer överens med den feedback vi har fått från konsumenter och branschexperter som klagat på Sinchs åtgärder mot bedragare.
- Vi är mycket oroade över att Sinch medvetet kan blunda för bedrägliga användare av sina tjänster. Även om grå marknadsverksamhet ofta verkar ekonomiskt attraktiv, introducerar den betydande risker som investerare kan undervärdera.
- Bluffsamtal är inga skämt utan en allvarlig fråga som förstör många liv. Offren för dessa bedrägerier är vanligtvis sårbara, ofta äldre personer, vilket i vår mening gör bedrägerierna särskiltäckliga och regulatoriskt skydd ännu viktigare.

IMPORTANT LEGAL DISCLAIMER

THIS REPORT AND ALL STATEMENTS CONTAINED HEREIN ARE THE OPINIONS OF GRIZZLY RESEARCH, AND ARE NOT STATEMENTS OF FACT.

Reports are based on generally available information, field research, inferences and deductions through Grizzly Research's due diligence and analytical process. Our opinions are held in good faith, and we have based them upon publicly available facts and evidence collected and analyzed including our understanding of representations made by the management of the companies we analyze, all of which we set out in our research reports to support our opinions, all of which we set out herein. HOWEVER, THEY REMAIN OUR OPINIONS AND BELIEFS ONLY.

We conducted research and analysis based on public information in a manner than any person could have done if they had been interested in doing so. You can publicly access any piece of evidence cited in this report or that we relied on to write this report.

Grizzly Research makes no representation, express or implied, as to the accuracy, timeliness, or completeness of any such information or with regard to the results to be obtained from its use.

We are entitled to our opinions and to the right to express such opinions in a public forum. We believe that the publication of our opinions and the underlying facts about the public companies we research is in the public interest, and that publication is justified due to the fact that public investors and the market are connected in a common interest in the true value and share price of the public companies we research. All expressions of opinion are subject to change without notice, Grizzly Research does not undertake a duty to update or supplement this report or any of the information contained herein.

Recipients of the research report are professional investors who are expected to make their own judgment as to any reliance that they place on the research report. You represent that you have sufficient investment sophistication to critically assess the information, analysis and opinion on this website.

You further agree that you will not communicate the contents of reports and other materials on this site to any other person unless that person has agreed to be bound by these Terms of Use. If you access this website, download or receive the contents of reports or other materials on this website on your own behalf, you agree to and shall be bound by these Terms of Use. If you access our website, download or receive the contents of reports or other materials on this website as an agent for any other person, you are binding your principal to these same Terms of Use.

As of the publication date of GRIZZLY RESEARCH LLC'S short-biased report, Certain GRIZZLY RESEARCH LLC Associated Persons (AS DEFINED HEREUNDER) (along with or through its members, partners, affiliates, employees, and/or consultants), clients, and investors, and/or their clients and investors have a short position in the securities of a Covered Issuer (and options, swaps, and other derivatives related to these securities), and therefore will realize significant gains in the event that the prices of a Covered Issuer's securities decline. Likely, you should assume that as of the publication date of any GRIZZLY RESEARCH LLC's long-biased report, certain GRIZZLY RESEARCH LLC Associated Persons, clients and investors, and/or their clients and investors have a material long position in all securities covered herein, and therefore stands to realize significant gains in the event that the price of any securities covered herein rises. Certain reports, whether long- or short-biased of a Covered Issuer, may also contain the opinions of other issuers in which GRIZZLY RESEARCH LLC Associated Persons, clients and investors, and/or their clients and investors may have a long position. Following publication of any long or short report, GRIZZLY RESEARCH LLC and GRIZZLY RESEARCH LLC Associated Persons are likely to continue to transact in Covered Issuers' securities for an indefinite period after an initial report on a Covered Issuer, and such position(s) may be long, short, or neutral at any time hereafter regardless of their initial position(s) and views as stated in GRIZZLY RESEARCH LLC'S research. One or more GRIZZLY RESEARCH LLC associated Persons have provided GRIZZLY RESEARCH LLC with publicly available information that GRIZZLY RESEARCH LLC has included in this report, following GRIZZLY RESEARCH LLC'S independent due diligence. YOU SHOULD DO YOUR OWN RESEARCH AND DUE DILIGENCE BEFORE MAKING ANY INVESTMENT DECISION WITH RESPECT TO THE SECURITIES COVERED HEREIN. THE OPINIONS EXPRESSED IN THIS REPORT ARE NOT INVESTMENT ADVICE NOR SHOULD THEY BE CONSTRUED AS INVESTMENT ADVICE OR ANY RECOMMENDATION OF ANY KIND. FOLLOWING PUBLICATION OF THIS REPORT, WE MAY CONTINUE TRANSACTING IN THE SECURITIES COVERED THEREIN, AND WE MAY BE LONG, SHORT, OR NEUTRAL AT ANY TIME HEREAFTER REGARDLESS OF OUR INITIAL OPINION.

To the best of our ability and belief, all information contained herein is accurate and reliable, and has been obtained from public sources we believe to be accurate and reliable, and who are not insiders or connected persons of the stock covered herein or who may otherwise owe any fiduciary duty or duty of confidentiality to the issuer. Note that Sinch AB and insiders, agents, and legal representatives of Sinch AB and other entities mentioned herein may be in possession of material non-public information that may be relevant to the matters discussed herein. Do not presume that any person or company mentioned herein has reviewed our report prior to its publication.

Introduktion

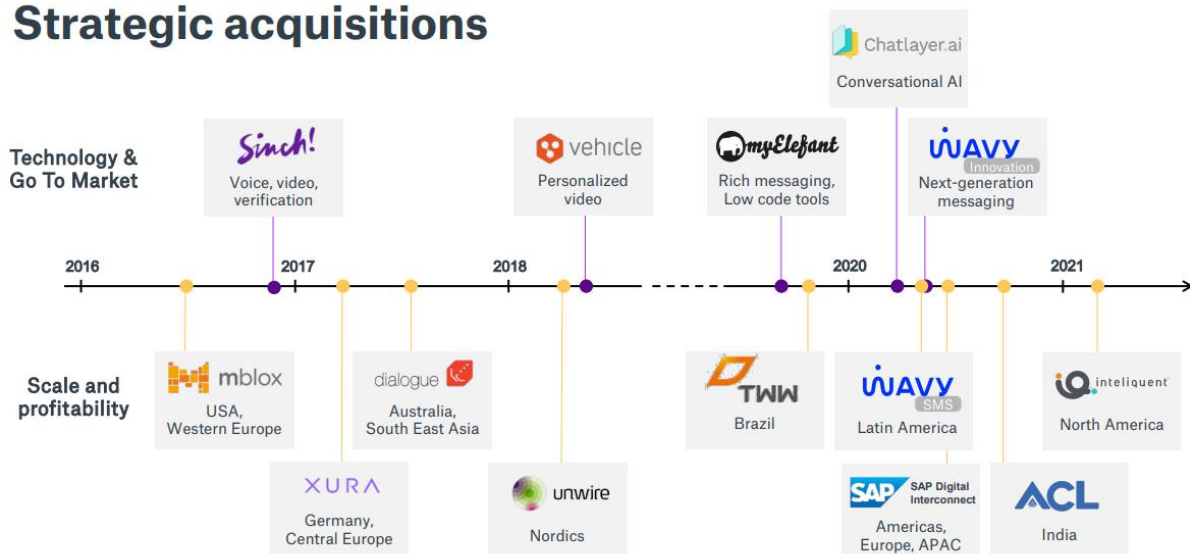
Sinch AB (tidigare CLX Communications AB) är en Sverige-baserad leverantör av molnkommunikationstjänster som verkar som en CPaaS (Communication Platform as a Service). Företaget genererar intäkter genom tre segment:

- API-plattform: Erbjuder meddelande-, e-post-, röst- och verifierings-API:er för tekniska team, inklusive hanteringsverktyg och integration med stora molnlösningar som Salesforce och Microsoft Teams.
- Applikationer: Utformad för företagsanvändare såsom marknadsförings- och kundframgångsteam, vilket eliminerar behovet av interna eller externa utvecklare.
- Nätverksanslutning: Förser telekomoperatörer och CSP:er med tjänster för att ansluta till Sinchs globala nätverk och hantera röst- och meddelandetrafik på ett effektivt sätt.

Företaget växte genom en sammanslagningsstrategi och slutförde alla sina förvärv i slutet av 2021.

Även om företaget har genomfört förvärv sedan [mitten av 2010-talet](#) har de flesta av dessa förvärv varit mindre till förvärvspriset och av kompletterande karaktär.

Strategic acquisitions



Källa: [Sinchs investerarpresentation februari 2021](#)

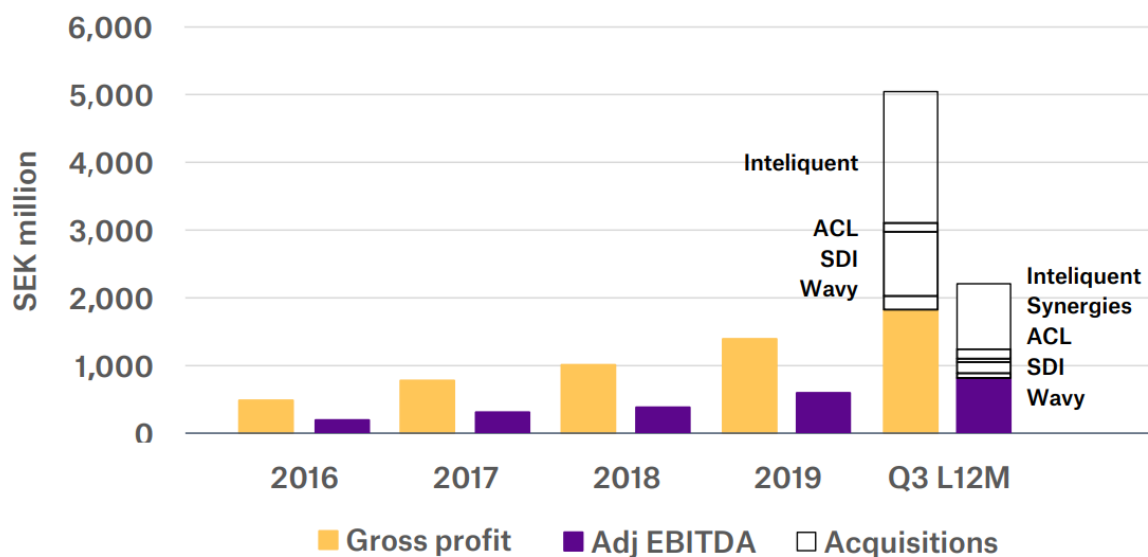
Företaget bytte namn till [Sinch AB i början av 2019](#) och uppgav att företaget "har använt handelsnamnet Sinch för sina realtidsröst- och videoprodukter sedan förvärvet av Sinch AB i

december 2016", vilket belyser det växande beroendet av API-segmentet, som då kallades realtidsröst- och videoprodukte.

Tydligen behövde Sinch en livlina, eftersom [CLX hade lånat ut 1,5 miljoner SEK](#) till Sinch genom ett konvertibelt lån för rörelsekapital. Dessutom verkar förvärvets enterprisevärde på 130 miljoner SEK billigt i jämförelse med de 900 miljoner SEK i intäkter som Sinch genererade 2016.

Inteliquent – Sinchs gyllene gås

I fortsättningen av sin förvävsstrategi slutförde företaget sitt största köp med [Inteliquent](#) i början av 2021 för en total ersättning på 1,14 miljarder USD. Inteliquent uppger att de är den största oberoende leverantören av röstkommunikation i USA. Vi anser att detta var det transformativa förvärvet som bidrog till att stärka Sinchs finansiella resultat under de följande åren.



Källa: [Sinchs investerarpresentation februari 2021](#)

Förvärvet tog större delen av 2021, med Sinch som tillkännagav förvärvet den 17 februari 2021 och slutligen avslutade affären i [december 2021](#).

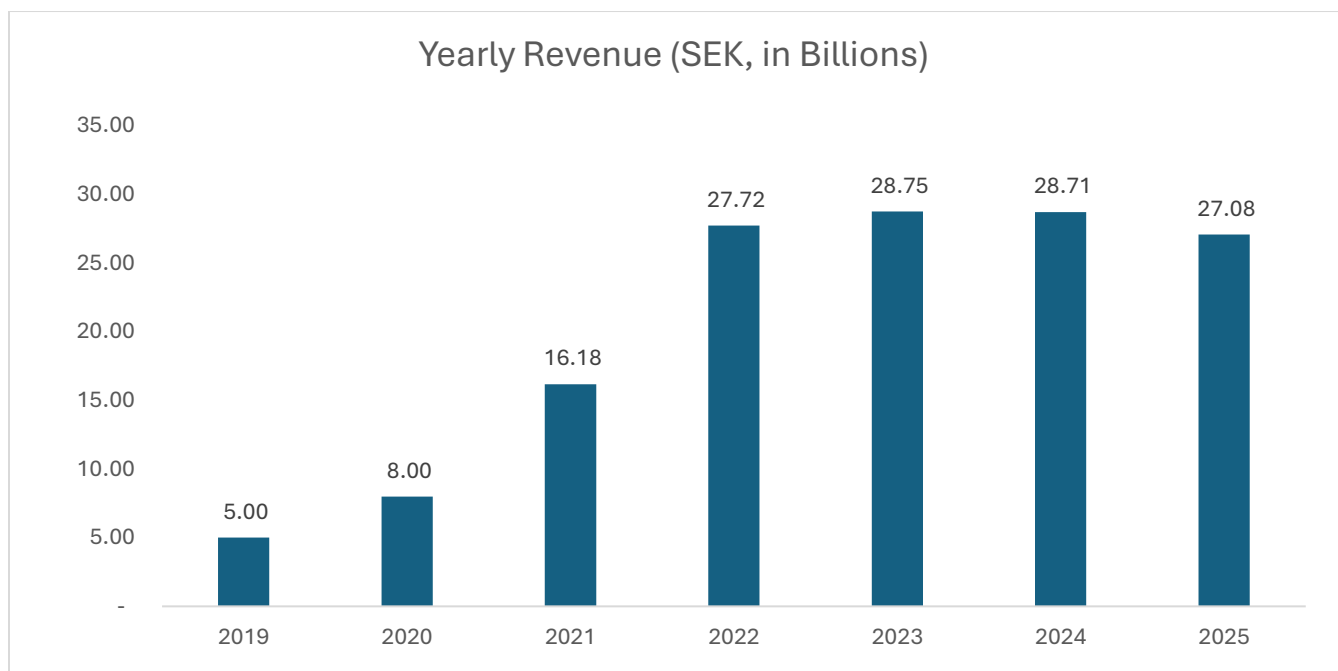
För att understryka vikten av detta förvärv uppgav företaget att Inteliquent-förvärvet

“gjorde Sinch till det största oberoende röstnätverket i USA. Inteliquent är en av de viktigaste ryggraden för alla leverantörer av röstsamtal i USA och är även betrodd av de stora amerikanska mobiloperatörerna för att driva deras person-till-person-samtal.”

Inteliquent och dess dotterbolag Onvoy och Neutral Tandem är inte traditionella mobiloperatörer. Snarare än att sälja telefonabonnemang direkt till konsumenter verkar företaget främst på grossistmarknaden för kommunikation och tillhandahåller den underliggande nätverksanslutningen som operatörer, molnkommunikationsplattformar och företag använder för att leverera telefonsamtal och textmeddelanden. Dess kunder inkluderar trådlösa operatörer, kabeloperatörer, VoIP-leverantörer och stora teknikplattformar som behöver tillförlitlig röstanslutning.

Det andra sättet som Inteliquent tjänar pengar på är genom att sälja telefonnummer i bulk till andra traditionella mobiloperatörer. Detta görs genom att Inteliquent förvärvar block av telefonnummer från numreringsmyndigheter. Inteliquent upprätthåller ett lager som täcker varje delstat och län i USA, vilket gör det möjligt för företaget att tillhandahålla nummer till kunder som behöver telefonnummer med specifika riktnummer.

Baserat på vår finansiella analys anser vi att Inteliquent är Sinchs gyllene gås. Även om Sinch inte redovisar intäkter per dotterbolag kan vi se att Sinchs finansiella resultat visar att de totala intäkterna ökade betydligt efter Inteliquent-förvärvet, från 16,17 miljarder SEK till 27,72 miljarder SEK. Av ökningen på 11,5 miljarder SEK stod Nordamerika för 8,8 miljarder SEK, eller ungefär 76% av den totala tillväxten.



Sammanställd från företagskällor

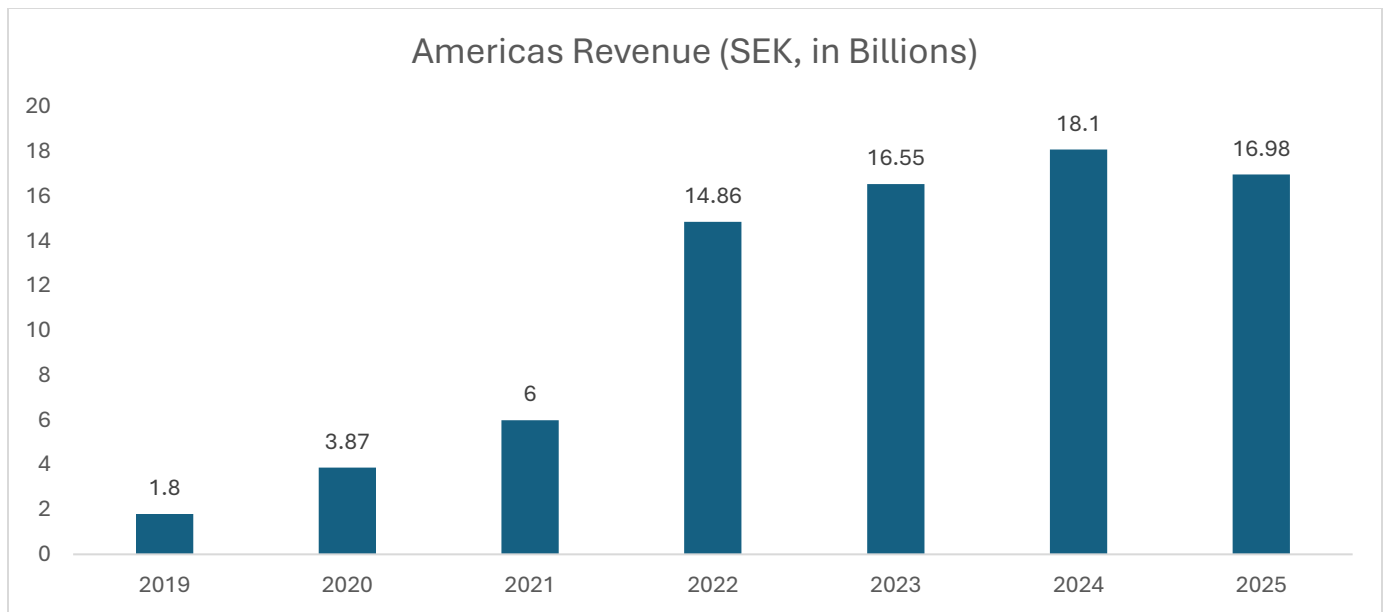
Enligt [Sinchs pressmeddelande](#) om förvärvet uppgav de att

“Under de tolv månaderna som avslutades den 31 december 2020 redovisade Inteliquent intäkter på 533 miljoner USD, bruttovinst på 256 miljoner USD, EBITDA på 135 miljoner USD och investeringar på 32 miljoner USD. Justerat för en Covid-relaterad uppgång som anses vara tillfällig

uppskattas intäkterna ha uppgått till cirka 499 miljoner USD, bruttovinsten till cirka 233 miljoner USD och den justerade EBITDA till cirka 112 miljoner USD.”

Under antagandet att Inteliquents verksamhet inte växte under två hela räkenskapsår motsvarar 553 miljoner USD ungefär 4,9 miljarder SEK, vilket skulle motsvara cirka 55% av ökningen på 8,8 miljarder SEK i nordamerikanska intäkter. Återigen under antagandet om 0% tillväxt under 2 hela år.

Med tanke på de segmenterade intäkterna mer än fördubblades intäkterna från Amerika från 6 miljarder SEK till 14,8 miljarder SEK år 2022, det första året då Inteliquents finansiella resultat var fullt konsoliderade i Sinchs finansiella redovisning.



Sammanställd från företagskällor

Till följd av förvärvet hoppade intäktsegmentet för Amerika från cirka 37% av de totala intäkterna till 53% av de totala intäkterna omedelbart efter Inteliquent-förvärvet och har fortsatt att växa till över 62% av Sinchs totala intäkter.

Dessutom har intäktstillväxten i Amerika generellt sett överträffat alla andra geografiska segment, vilket tyder på att det är företagets viktigaste intäktsegment.

	2019	2020	2021	2022	2023	2024	2025
America YoY Growth		114.17%	56.20%	145.61%	11.33%	9.39%	-6.23%
Non-USA YoY Growth		28.57%	144.08%	26.96%	-5.15%	-13.03%	-4.74%

**Inteliquent FY Revenue Incorporated*

Sammanställd från företagskällor

Varför vi anser att Sinch spelar en stor roll i att möjliggöra bluffsamtal

Vi undersökte Sinch, dess dotterbolag och jämförde praxis med branschkonkurrenter. Vår slutsats är tydlig. Vi anser att Sinchs tjänster används för att genomföra den största andelen bluffsamtal och robotsamtal i USA.

Vi baserar våra slutsatser på vår undersökning som granskar Sinch från fyra olika vinklar: konsumentupplevelsen, det regulatoriska landskapet, branschexperternas synpunkter och företagets interna perspektiv.

Sinch möter ökad regulatorisk granskning

I maj 2022, månader efter att Sinch avslutade förvärvet av Inteliquent, skickade den amerikanska Federal Trade Commission (FTC) ett varningsbrev till [Inteliquent](#), där det angavs att företaget underlättade olagliga robotsamtal som härstammade från utländska bluffoperationer.

Det åttasidiga dokumentet konstaterade:

“ITG [USTelecoms Industry Traceback Group] har tidigare meddelat er om dessa samtal och gett er tillgång till stöddata som identifierar varje samtal - inklusive en inspelning av det olagliga robotsamtalet” och att “de många spårningsmeddelanden riktade till Inteliquent, Inc. indikerar att ni tydligt vidarebefordrar och överför olaglig robotsamtalstrafik medvetet.” — Maj 2022, FTC:s varningsbrev

Det verkar som att de tidiga varningstecknen på Inteliquents otillräckliga kapacitet för bedrägeri- och missbruksdetektering redan var uppenbara.

Sedan genomförde Social Security Administration Office of the Inspector General år 2023 en utredning kallad "[Operation Upstream Carrier Without a Paddle](#)" som syftade till att fastställa huruvida gateway-telekomleverantörer tillät bedräglig robotsamtalstrafik att passera genom sina nätverk samtidigt som de tjänade avgifter på den trafiken. De utfärdade en stämning mot Inteliquent och nådde slutligen ett förlikningsavtal med företaget som betalade ett litet civilrättsligt böter.

Samtidigt fick Sinch uppmärksamhet från regulatorer utanför USA. I maj 2023 fann en [rapport](#) från Australian Communications and Media Authority (ACMA) att Sinchs australienska dotterbolag Sinch Australia Pty Ltd (Sinch) "tillät SMS att skickas med textbaserade avsändar-ID:n utan tillräckliga kontroller för att säkerställa att de användes legitimt."

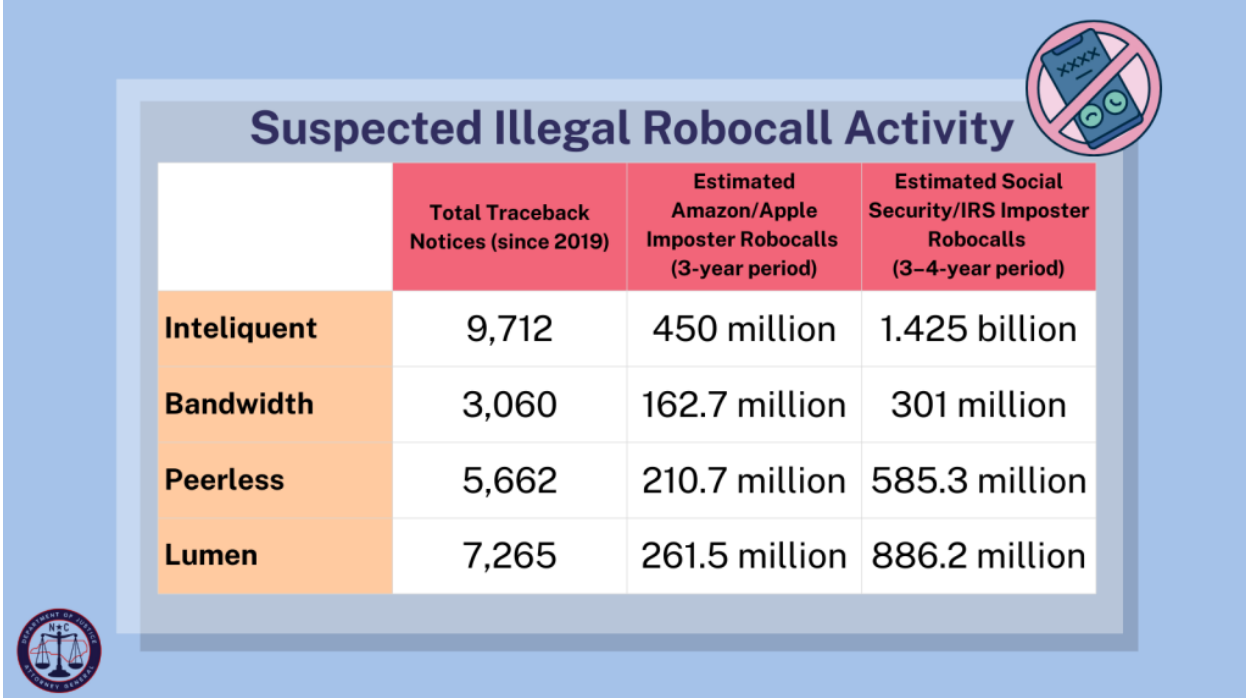
Vi anser att den mest betydande regulatoriska undersökningen som hotar Sinchs verksamhet är [Anti-Robocall Multistate Task Force](#), ledd av justitieministrarna i Indiana, North Carolina och Ohio men som inkluderar alla delstaters justitieministrar. Den tvärpolitiska arbetsgruppen undersöker för närvarande Inteliquent för att påstås möjliggöra nästan 50% av alla robotsamtal i USA. Uttalandena från justitieministrarnas kontor antyder att Sinch och dess dotterbolag är den enskilt största möjliggöraren av robotsamtal i USA. Det senaste meddelandet om utredningen från december 2025 tyder på att utredningen intensifieras.

Arbetsgruppens meddelande varnade Inteliquent för att det överförde "miljarder bedrägliga robotsamtal" och beordrade det att sluta vidarebefordra olaglig trafik.

I det åttasidiga meddelandet som skickades till [Inteliquent](#) noterade arbetsgruppen att av de 9 712 spåringsmeddelanden som skickats till Inteliquent sedan 2019,

"Minst 5 728 av dessa spåringsmeddelanden skickades till Inteliquent efter augusti 2022, vilket är efter att arbetsgruppen först kontaktade om sina farhågor gällande Inteliquents samtalstrafik, och meddelanden utfärdas fortfarande 2025." – December 2025, justitieministrarnas brev

Ett spåringsmeddelande är en officiell varning från branschutredare som indikerar att ett företag har överfört ett samtal kopplat till en misstänkt olaglig robotsamtalskampanj.



The table is titled "Suspected Illegal Robocall Activity" and is set against a light blue background. In the top right corner, there is a circular icon with a red border and a diagonal slash, containing a smartphone with a green checkmark and a red 'X' over it, representing a prohibition on robocalls. The table has four columns: the first column lists the entities, and the next three columns list metrics. The rows are Inteliquent, Bandwidth, Peerless, and Lumen. Inteliquent's row is highlighted in orange. In the bottom left corner of the table area, there is a small circular seal for the North Carolina Department of Justice, featuring a scale of justice and the text "N.C. DEPARTMENT OF JUSTICE".

	Total Traceback Notices (since 2019)	Estimated Amazon/Apple Imposter Robocalls (3-year period)	Estimated Social Security/IRS Imposter Robocalls (3-4-year period)
Inteliquent	9,712	450 million	1.425 billion
Bandwidth	3,060	162.7 million	301 million
Peerless	5,662	210.7 million	585.3 million
Lumen	7,265	261.5 million	886.2 million

Källa: [Pressmeddelande från justitieminister Jeff Jackson](#)

Enligt meddelandet är Inteliquent ansvarigt för ungefär 45% av det totala antalet Amazon-, Apple- och myndighetsimponatörsrobotsamtal som mäts av arbetsgruppen. Vi anser att detta är ett löjligt högt antal.

	Inteliquent		
	Sample Size	Involvement	% of Total
Amazon/Apple Imposter Robocalls	2,000,000	900,700	45.04%
SSA/IRS Government Imposter Robocalls	6,200,000	2,850,000	45.97%

Källa: [Sammanställt utifrån det åttasidiga föreläggandet](#)

Arbetsgruppens meddelande anger:

“Vidare bedömdes en analys av en del av Inteliquents sannolika inblandning i dirigeringen av nationell samtalstrafik gällande Amazon/Apple-impostörrobotsamtal. Mellan oktober 2021 och november 2024, bland ett nationellt urval av cirka 2 miljoner transkriberade och inspelade Amazon/Apple-impostörrobotsamtal, uppskattades över 900 700 av dessa Amazon/Apple-impostörrobotsamtal ha underlättats av Inteliquent. Således, av de över 1 miljard uppskattade Amazon/Apple-impostörrobotsamtal som nådde konsumenter över hela landet i detta urval under denna period, uppskattades cirka 450 miljoner av dessa bluffrobotsamtal ha underlättats av Inteliquent.” – December 2025, justitieministrarnas brev

Och

“En liknande analys av Inteliquents sannolika inblandning i dirigeringen av nationell samtalstrafik gällande SSA/IRS-myndighetsimpostörrobotsamtal bedömdes. Mellan maj 2020 och november 2024, bland ett nationellt urval av cirka 6,2 miljoner transkriberade och inspelade SSA/IRS-myndighetsimpostörrobotsamtal, uppskattades mer än 2,85 miljoner av dessa SSA/IRS-myndighetsimpostörrobotsamtal ha underlättats av Inteliquent. Således, av de över 3,1 miljarder uppskattade SSA/IRS-myndighetsimpostörrobotsamtal som nådde konsumenter över hela landet i detta urval under denna period, uppskattades cirka 1,425 miljarder av dessa bluffrobotsamtal ha underlättats av Inteliquent.” – December 2025, justitieministrarnas brev

Andra källor rapporterar siffror som är ännu högre än de som citeras av Industry Traceback Group (ITG) och justitieministrarna i deras formella meddelanden.

År 2022 väcktes en grupptalan mot [Inteliquent och Onvoy](#), där företagen anklagades för att ha underlåtit att vidta tillräckliga åtgärder för att stoppa robotsamtal riktade till federala studielåntagare. Kärna i denna rättegång var personer som tog emot robotsamtal och direkta röstmeddelanden innehållande förinspelat, vilseledande och missledande innehåll. Dessa meddelanden innehöll artificiella röster och skickades till deras telefoner med hjälp av "spoofade" telefonnummer utformade för att dölja det sanna ursprunget för samtalen.

Kär a н д ena hävdar att cirka 60% av alla robotsamtal och skräppostsamtal som rings i USA dirigeras genom Onvoy-nätverket till amerikanska konsumenters telefoner. Detta påstående understryker omfattningen av Inteliquents och Onvoys inblandning i överföringen av oönskade och potentiellt bedrägliga kommunikationer.

"Baserat på information och övertygelse levereras 60% av alla skräpposttelefonsamtal i USA till konsumenters telefoner via Onvoys nätverk. Baserat på information, övertygelse och advokatundersökning levereras cirka 60% av alla robotsamtal som rings i USA av Onvoy-nätverket till amerikanska konsumenters telefoner." Utdrag från grupptalan 2022

[Kär a н д ena avvisade frivilligt stämningen](#), vilket vi tolkar som en indikation på att ärendet troligen löstes utanför domstol, vilket gjorde det möjligt för Inteliquent och Onvoy att undvika att erkänna ansvar.

Siffrorna ovan pekar tydligt ut Sinch som den mest framträdande möjliggöraren av bluffsamtal.

Med tanke på [YouMails Robocall Index](#) ser vi att det förekom [52,8](#) miljarder och [52,5](#) miljarder robotsamtal i USA under 2024 respektive 2025. Detta tyder på att om siffrorna i grupptalan är korrekta, kan Inteliquent behandla över 23 miljarder bedrägliga telefonsamtal på sitt nätverk årligen. Denna siffra återspeglar endast robotsamtal och exkluderar bedrägeri- eller nätfiskerelaterade samtal, samt eventuella skräppost-textmeddelanden.

Det är anmärkningsvärt att Sinch inte har redovisat någon av dessa regulatoriska frågor i sina rapporter, inklusive meddelandet från Anti Robocall Task Force från december 2025. Kommunikationsutbytet visar att Inteliquent har haft en löpande dialog med arbetsgruppen, vilket tyder på att bolaget haft tillräckliga möjligheter att lämna lämpliga upplysningar till investerare om granskningen och dess omfattning.

Den mest missbrukade CPaaS-leverantören enligt konsumenter

Sedan förvärvet av Inteliquent har Sinch och dess dotterbolag, enligt vår analys, varit de mest frekvent klagade på företagen i branschen.

Vår analys bygger på två datakällor: onlineforum där bluffspårare och privatpersoner rapporterar telefonnummer som används i bedrägerier, samt webbplatser för telefonnummeruppslagning där användare kan markera nummer som skräppost eller bedrägliga.

Ett av de mer framträdande forum vi identifierade är Scammer.Info, ett meddelandebrädsforum där användare rapporterar, diskuterar och delar information om skräppost och bedrägliga uppringare. ScamWarners.com och ScamSurvivors.com tjänar ett liknande syfte och erbjuder jämförbara forum inriktade på att rapportera och diskutera bluffrelaterad aktivitet.

När vi sökte på dessa webbplatser efter nyckelord relaterade till Sinch och dess dotterbolag och jämförde det med konkurrenter, finner vi att Sinch har ett betydligt högre antal resultat med över 800 jämfört med Twilio som hade 450 resultat.

	Scammer.Info	r/ScamNumbers	r/Scams	ScamWarners	ScamSurvivors
Sinch	800	90	25	325	467
Twilio	~500	12	3	17	32
Peerless Network	242	3	1	20	138
Telnyx	338	14	2	3	7

På några av de mer populära bedrägeri-relaterade subreddits, såsom r/ScamNumbers och r/Scams, är resultaten konsekventa. Det finns betydligt fler inlägg relaterade till personer som tar emot bluffsamtal eller textmeddelanden från telefonnummer associerade med Sinch och dess dotterbolag.

Vidare visar en analys gjord på webbplatser för telefonnummeruppslagning att Sinch och dess dotterbolag konstant flaggas och slås upp av privatpersoner i en högre takt än deras konkurrenter.

	NumberGuru	800Notes	WhoCallsMe	TrueCaller
Sinch	573	296	8	222
Twilio	45	4	5	212
Peerless Network	268	108	6	208
Telnyx	267	19	0	211

Att göra samma analys men begränsa sökresultaten till det senaste året visar att resultaten för konkurrenter minskade väsentligt, vilket tyder på att deras konkurrenter fokuserar på att minska bluffsamtal i sitt nätverk.

Last Twelve Months	NumberGuru	800Notes	WhoCallsMe	TrueCaller
Sinch	490	17	5	208
Twilio	2	2	0	6
Peerless Network	130	2	0	4
Telnyx	45	0	0	2

Vi utvecklade ett index som viktar dessa resultat baserat på varje företags uppskattade marknadsandel över 5%, enligt [Metrigy](#). Detta möjliggör en mer jämförbar analys av den relativa

exponeringen för varje CPaaS-leverantör mot skräppostsamtalsaktivitet. Detta visar återigen att Sinch rankas betydligt högre än sina konkurrenter. Vi anser att detta är en rättvis och lämplig jämförelse, eftersom alla företag verkar inom CPaaS-sektorn.

	Market Share	NumberGuru Index	800Notes Index	WhoCalls Me Index	TrueCaller Index
Sinch	12%	39.52	1.37	0.40	16.77
Twilio	25%	0.08	0.08	0.00	0.24
Peerless Network	14%	9.29	0.14	0.00	0.29

**All companies with above 5% market share in CPaaS*

Några ytterligare individuella exempel: ett inlägg på [Twitter/X](#) visar att Onvoys system användes för att skicka ut rasistiska textmeddelanden till svarta personer dagen efter det amerikanska valet 2024. Detta visar hur vittomfattande Inteliquent/Onvoy-nätverket är.

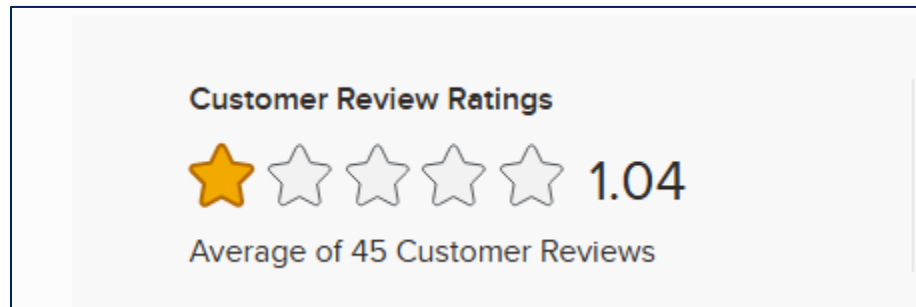
Diskussioner i Reddit-gemenskapen r/ScamNumbers väcker frågan: "[Varför använder alla bedragare SINCH?](#)" En användare förklarade,

"Sinch har ett dåligt rykte inom VOIP-grossistsektorn. De tenderar att ignorera rapporter om bedrägligt eller kriminellt beteende av sina kunder och väljer istället att sälja stora mängder nummer för vinst. Även populära appar som TextNow förlitar sig på Sinch-nummer, vilket bedragare ibland utnyttjar."


[Scammer.Info](#) är värd för flera inlägg som diskuterar Sinch, Inteliquent, Onvoy och Neutral Tandem. Vissa inlägg är ganska detaljerade och ger insikt i de omfattande ansträngningar som bluffjakare gör för att ta bort telefonnummer från Sinchs nätverk. Till exempel beskriver ett inlägg från december 2023 med titeln "[Sinch: Fraud Support Experience \(Case Study\)](#)" inläggsskrivarens erfarenhet med Sinch:






"Enligt min erfarenhet har Sinchs kundsupport gällande bedrägerianmälningar - oavsett om de skickats via e-post eller webbformulär - varit nedslående. Varken Sinch eller dess grossister erbjuder konsumenter uppdateringar om ärenden som lämnats in via deras webbformulär."

När man tittar på [Inteliquents BBB](#)-sida har företaget 1,04 stjärnor av 5 och har flera klagomål, där många recensioner beskriver företaget som den största förövaren av bluffsamtal.









Vissa av dessa klagomål beskriver personer som är registrerade i det nationella registret för samtalsspärr (National Do Not Call Registry) men som fortsätter att ta emot skräppostsamtal från nummer associerade med Inteliquents telefonnummer eller Onvoy-nätverket.

 **Ebony B**
Date: 11/03/2025


    






this company calls me everyday non stop consistently. I have asked them to put me on the DO NOT CALL list. The person on the phone told me that they will call me until they get tired. So ONVOY i am seeking legal action at this point of being consistently harassed.

 **Dan M**
Date: 02/27/2026

I am receiving several unsolicited calls a day from phone numbers registered to this company.

 **Lindsey J**
Date: 01/30/2026

This company has called me 4 times today, with 4 different numbers claiming to be reaching me about "my car's extended warranty." I did not answer the first 3 and blocked and reported the number for spam. The 4th call I did answer and instructed them to not call again. The number is some iteration of 785-212-xxxx. Absolutely ridiculous to be harassing me 4 times in one day, and all from different generated phone numbers.

Sinch ur perspektivet av branschexperter och bluffjakare

Vi konsulterade branschexperter som beskrev för oss ett mönster av missbruk relaterat till Sinchs dotterbolag Inteliquent och Onvoy. Sinch verkar vara uppbyggt för att möjliggöra bluff- och robotuppringare samtidigt som det försvårar för konsumenter att varna Sinch om de bedrägerier eller robotsamtal som görs i deras nätverk. Sinch har ett enda [webbformulär](#) för att rapportera missbruk och svarar inte på eller kommunicerar via sina e-postadresser för bedrägerirapportering om man kontaktar dem direkt.

Detta fungerar endast eftersom Sinch ibland har lager emellan sig själv och den slutliga användaren som missbrukar tjänster för bluffsamtal. Sinch säljer sina tjänster i stora paket till företag, såsom Verizon eller AT&T, som sedan i sin tur kan sälja tjänsten till illegitima slutanvändare. Detta förändrar inte det faktum att det ligger inom Sinchs makt att stoppa missbruket.

Vi vill lyfta fram en offentlig branschexpertrapport som vi fann särskilt övertygande.

En grupp aktivistiska bluffjakare som kallar sig Demurrage publicerade nyligen ett nästan 200-sidigt dokument med titeln "[Sinch: A Closer Look At Consistent Avoidance & Lack of Communication \(A Case Study Conducted By The Demurrage Team\)](#)." Denna nya rapport, daterad december 2025, är uppföljaren till en rapport från 2024 med titeln "Sinch: A Case Study."

Rapporten anger att:

"Den ursprungliga rapporten dokumenterade block av nummer på Onvoy-nätverket som användes för att underlätta Spectrum och senare Xfinity kundsupportbedrägerier, alla förvärvade av bedragare som opererade från illegala callcenter i Pakistan. Den belyste Sinchs brist på kommunikation, begränsningarna i dess enda rapporteringsmetod, Sinch-webbformuläret, och jämförde det med andra telekomleverantörer som agerade snabbt och erbjöd tillgängliga rapporteringskanaler till den genomsnittlige konsumenten. Denna uppdaterade rapport bekräftar att de problem som identifierades 2024 förblir olösta." December 2025, Demurrage-rapporten

Rapporten innehåller hundratals skärmdumpar som exponerar företaget genom att visa att Sinch fortsätter att tillåta dessa illvilliga aktörer på sin plattform. Demurrage förklarar vidare hur dåligt Sinch hanterar rapportering av dessa bedrägliga nummer till företaget. Demurrage uppger att de försökte rapportera "ett PayPal-återbetalningsbedrägeri som involverade ett MS Teams-nummer, med hjälp av e-postadressen fraudoperations@sinch.com. En skärmdump och en inspelning av bedragaren som svarade på samtalet inkluderades." Sinch brydde sig inte ens om att svara på deras meddelande. Demurrage säger att detta står i direkt motsättning till hur andra telekomleverantörer

som Lumen agerar, om vilka de säger att de "omedelbart lägger en tillfällig blockering på ett rapporterat nummer innan ärendet vidarebefordras till grossisten." Lumen kommunicerar med konsumenter under hela processen och löser vanligtvis bedräglig trafik inom minuter.

Demurrages team fick till slut ett svar som var mer än oroande för dem. Sinchs bedrägerioperationer svarade och sa att numret är associerat med "ett större volymproblem med en enskild kund." Detta antyder att Sinch inte genomförde en ordentlig KYC-kontroll och i slutändan sålde ett block av telefonnummer till någon som senare använde dem i försök till bedrägerier.

Ett annat problem som Demurrage-rapporten lyfter fram är VOIP-leverantörerna som använder antingen Inteliquent- eller Onvoy-nätverket. Deras rapport bekräftar att en av de "minst responsiva leverantörerna på Sinch-nätverket när det gäller att hantera bedrägeri" i Talkatone använder Onvoy-nätverket för att koppla sina samtal.

Enligt deras egen webbplats är [Talkatone](#) en gratis VoIP-app för iOS och Android som tillhandahåller ett dedikerat amerikanskt eller kanadensiskt telefonnummer, vilket gör det möjligt för användare att ringa och skicka textmeddelanden obegränsat och kostnadsfritt via Wi-Fi till dessa regioner.

Istället för att Talkatone vidtar åtgärder eller vidarebefordrar bedräglig aktivitet till Sinch, "nekar företaget rutinmässigt ägandeskapet av rapporterade nummer och vägrar att agera, med påståendet att ospecificerade 'lagar' hindrar det från att stänga av bedrägliga nummer" och berättar för användaren att de måste ha lämnat in ett rättsligt anspråk innan någon utredning kan äga rum.

Detta illustrerar vad vi menar när vi säger att företaget kan ha flera lager mellan sig självt och slutanvändaren, vilket gör det möjligt för Sinch att avleda ansvaret till mellanhänder som Talkatone för otillräckliga KYC-metoder. Enligt vår uppfattning borde Sinch inta en mer proaktiv hållning genom att avsluta åtkomsten för alla användare som missbrukar dess nätverk. Som den största leverantören av röstkommunikation skulle vi förvänta oss att företaget upprätthåller robusta och välresurserade funktioner för bedrägeribekämpning, efterlevnad och KYC/KYT.

Vi vill avsluta denna del med två citat från slutsatsen i Demurrage-rapporten,

"Tiden för varningar har passerat. Sinch måste ta itu med dessa problem direkt. Företaget behöver en övervakad, dedikerad e-postkanal för bedrägerianmälningar och måste upprätthålla öppen kommunikation med konsumenter angående status och resultat av deras anmälningar. Många av Sinchs konkurrenter gör redan detta, och det finns ingen motivering för Sinchs fortsatta brist på engagemang." December 2025, Demurrage-rapporten

Och

“Sinch har blivit den mest frekvent missbrukade telekomleverantören för bedragares återuppringsnummer, och utan omfattande reformer kommer detta problem endast att förvärras under 2026 och framåt.” December 2025, Demurrage-rapporten

Sinchs efterlevnadsteam är nästan obefintligt

Vi frågade tidigare anställda och branschexperter om Sinchs efterlevnadspolicyer. Vi möttes av flera negativa kommentarer; en expert berättade för oss att Inteliquent, Onvoy och Neutral Tandem länge har varit de värsta inom bluffrapporteringsgemenskapen, och bluffjakare klagar rutinmässigt mer på dessa enheter än på något annat involverat företag.

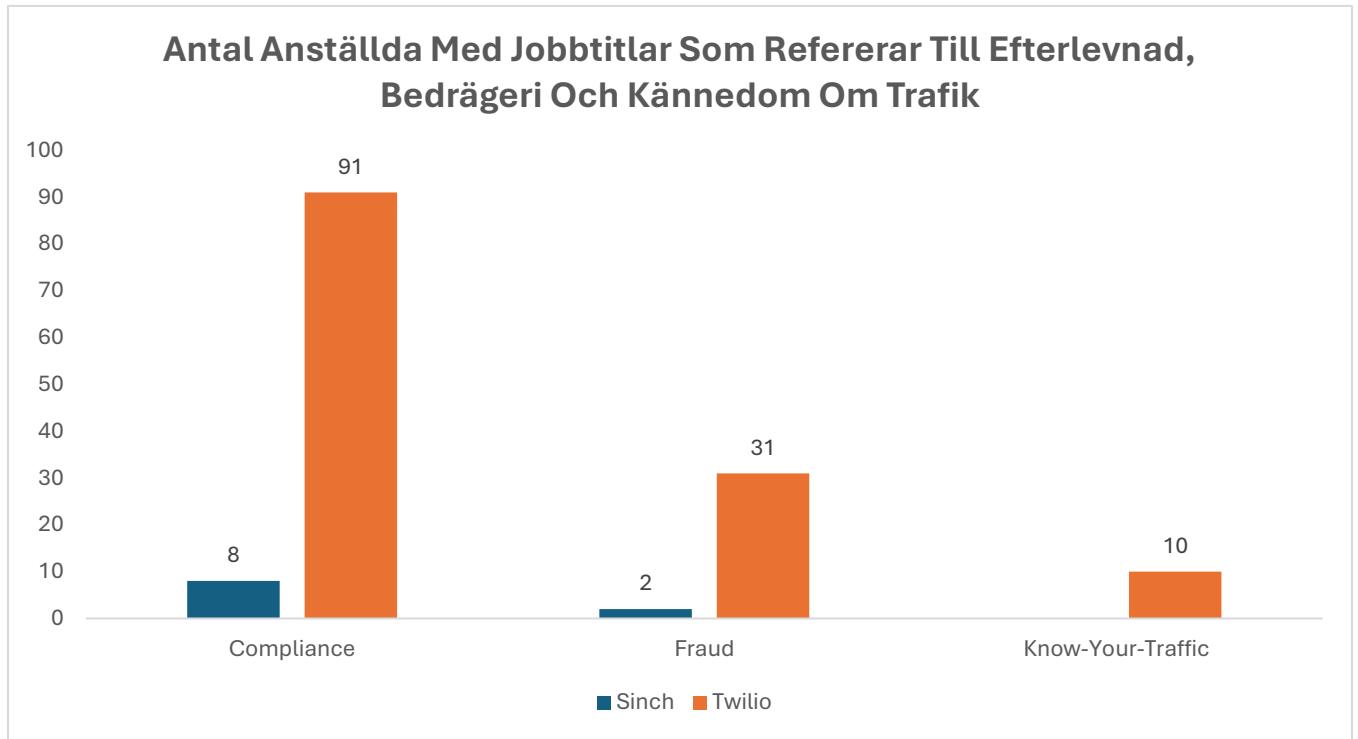
En tidigare anställd, som arbetade på Inteliquent när det var ett fristående företag, uppgav att det endast var en eller två personer som arbetade med efterlevnadsfrågor. Experter noterade också att Sinch, bland de andra CPaaS-företagen, skulle använda sig av branschens efterlevnadsgrupper vid behov.

Vi fann dessa kommentarer intressanta, eftersom Inteliquent enligt egen utsago är den "största oberoende leverantören av röstkommunikation i USA." Vi skulle förvänta oss att företaget har robusta team för efterlevnad, bedrägeridetektering och kundkännedom/trafikhantering som är tillräckliga för dess storlek.

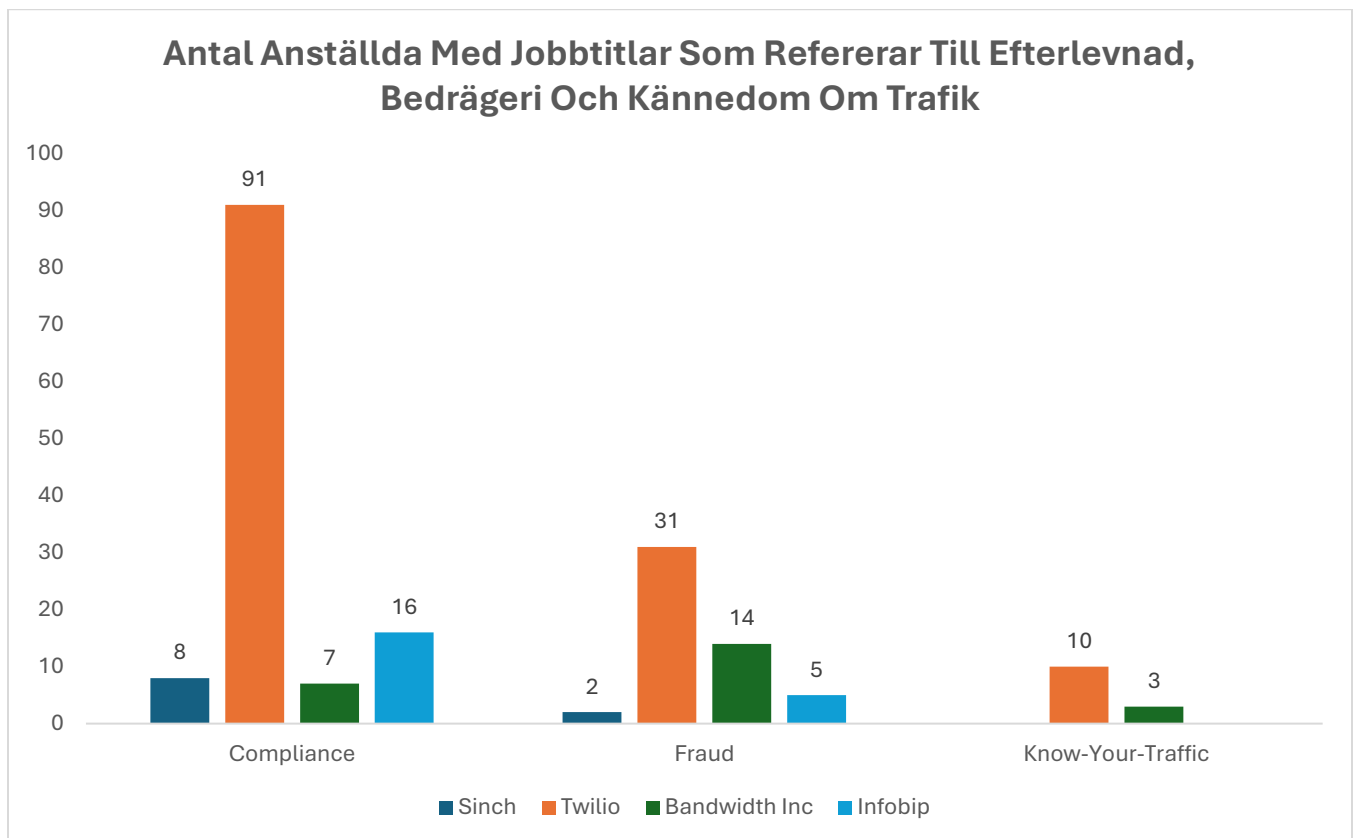
Till vår förvåning resulterade en omfattande sökning på LinkedIn SalesNavigator efter personer som arbetar för Sinch med jobbtitlar relaterade till bedrägeri, KYC eller efterlevnad i endast 20 personer. Tydligen bestod efterlevnadsteamet av endast cirka 8 personer, medan de övriga 12 personerna verkade ha enstaka roller i företaget. Dessutom sökte vi efter Inteliquent-anställda med samma nyckelordssökning, men vi fann inga resultat.

Vi jämförde våra resultat med Sinchs [största konkurrent](#), Twilio. Även om Twilio genererar ungefär dubbelt så stora intäkter anser vi att detta fortfarande är en lämplig jämförelse, eftersom Sinch skulle förväntas anställa fler personal inom efterlevnad, bedrägeri och KYC-funktioner, med tanke på sin position inom CPaaS tillsammans med Inteliquents roll som den största grossistleverantören av röstsammankoppling och infrastruktur i USA.

Twilio har ett betydligt större totalt antal anställda med jobbtitlar relaterade till bedrägeri, KYC eller efterlevnad med 149 personer. Twilio har flera storskaliga team för var och en av dessa divisioner. Twilio hade över 91 anställda med jobbtitlar som refererar till efterlevnad och nästan ett dedikerat efterlevnadsteam på 55 personer.



När vi utvidgade vår analys till att inkludera andra jämförbara företag såsom Infobip och Bandwidth Inc. observerade vi att de hade ett liknande antal anställda i varje kategori men fortfarande ett högre totalt antal anställda än Sinch som arbetar i någon form av bedrägeri-, KYC- eller efterlevnadsroll.



Vi anser att, som ett företag som i praktiken kontrollerar en kritisk del av telekommunikationsmotorvägen och som har en konkurrenskraftig andel inom CPaaS-sektorn, bör standarden för efterlevnad, bedrägeriförebyggande och kundkännedom/trafikteam vara väsentligt högre än den hos dess konkurrenter.

Dessa datapunkter stämmer överens med de erfarenheter som beskrivs av kunder och branschexperter som påpekar att Sinch är märkbart långsam med att hantera bedrägeribekymmer. Vi finner Sinchs efterlevnadsinsatser fullständigt otillräckliga. Vi anser att kontrollerna kan vara otillräckliga av design, eftersom Inteliquent verkar tjäna betydande belopp på olaglig bluff- och robotsamtalsverksamhet genom att sälja block av telefonnummer till illvilliga aktörer och dirigera de samtal de genererar. Det är en olycklig affärsverklighet att tillgodose kunder i gråzonen eller illegala kunder ofta har de bästa vinstmarginalerna.

Med tanke på Sinchs betydande marknadsandel inom CPaaS-sektorn, och skalan av Inteliquent och Onvoy som ledande grossistleverantörer av röstsammankoppling och infrastruktur i USA, skulle vi förvänta oss att företaget och dess dotterbolag är bland de mer frekvent utsatta plattformarna för missbruk. Detta skulle i sin tur lägga tonvikt på efterlevnad, bedrägeribekämpning och kundkännedomsroller. Vår analys visar dock att företaget verkar lägga relativt begränsat fokus på dessa roller.

Vi förväntar oss att Sinch kommer att försöka motbevisa våra resultat med argumentet att de i hög grad förlitar sig på branschpartners och därför inte behöver ett stort internt team. Detta ställningstagande verkar dock tveksamt, eftersom Inteliquents efterlevnadsmekanismer åtminstone verkar ineffektiva. Vi skulle förvänta oss ett dedikerat internt efterlevnadsteam jämförbart med Twilios.

Vi ser att Sinch ofta hänvisar till sin efterlevnad av STIR/SHAKEN-reglerna, ett ramverk som introducerades av FCC år 2022 och som kräver att samtal digitalt signeras med en attesteringsnivå (A, B eller C). Efter konsultation med branschexperter anser vi att STIR/SHAKEN-efterlevnad inte skyddar Sinch från rättsliga konsekvenser och inte förändrar det faktum att det ligger inom Sinchs makt att övervaka den bedrägliga trafiken.

Bluffsamtal är ingen skämtsam fråga

Enligt [FTC](#) har bedrägerier blivit en nästan 16 miljarder dollar stor industri i USA och fortsätter att växa, enligt Lois Greisman, biträdande direktör för FTC:s avdelning för marknadsföringspraxis. Denna siffra representerar en betydande ökning jämfört med föregående år, som såg 2,6 miljoner

bedrägerirapporter och över 12 miljarder dollar i rapporterade förluster. Sedan 2020 har rapporterade bedrägeriförluster ökat med cirka 430%.

Bedrägerier med falska identiteter utgjorde mer än 3,5 miljarder dollar, eller 22% av de totala rapporterade förlusterna, vilket gjorde dem till den mest frekvent rapporterade typen av bedrägeri. Det är troligt att dessa siffror underskattar den verkliga omfattningen av förlusterna, eftersom många offer kan vara ovilliga att rapportera incidenter på grund av skamkänslor.

Data sammanställd av [Commsrisk](#) från FTC indikerar att bedrägerirelaterade förluster via telefonsamtal och textmeddelanden fortsätter att öka och nådde 540 miljoner dollar under det tredje kvartalet 2025.

En enkel sökning på Google eller YouTube avslöjar många fall av personer som förlorat sina livsbesparingar genom telefon- och textbedrägerier. [Ett av de vanligaste bedrägerierna är mormorsbedrägeriet](#). Det riktar sig mot äldre personer där bedragare ringer och låtsas vara ett barnbarn i trubbel, och hävdar vanligtvis att de är arresterade, skadade eller strandsatta och tigger desperat om pengar. Bedragarna säger ofta något vagt som "det är jag!" och låter mor- eller farföräldrarna själva ange namnet. Den viktigaste manipulationen är ett krav på sekretess ("berätta inte för mamma och pappa"), vilket hindrar offret från att verifiera historien. Med betalning begärd genom ospårbara metoder som presentkort eller banköverföringar.

År 2025 greps av [RCMP](#) en individ som misstänks vara ledaren för ett mormorsbedrägerinätverk, som enligt uppgift är ansvarig för olagliga vinster på över 30 miljoner dollar från amerikanska seniorer.

En Reddit-användare berättade att hans mormor förlorade cirka 40 000 dollar efter att ha svarat på ett bedrägligt textmeddelande om ett komprometterat konto. En [CBC-artikel](#) belyste ett fall där en äldre person förlorade nästan 800 000 kanadensiska dollar efter ett popup-datorbedrägeri och efterföljande bedrägliga telefonsamtal.

Vår poäng är att offren vanligtvis är sårbara personer, särskilt äldre, vilket gör denna situation särskilt äcklig.

Slutsats

Sinch AB har utvecklats till en av de största möjliggörarna av bluffsamtal i västra halvklotet genom sitt ägande av Inteliquent. Trots de till synes attraktiva finansiella resultaten som genereras av denna verksamhet står företaget inför intensifierad regulatorisk granskning, otillräckliga efterlevnadskontroller och växande skador på sitt rykte.

Vi anser att regulatorer nu stänger in sig, med meningsfulla verkställighetsåtgärder som sannolikt kommer inom den närmaste framtiden. Sådana ingripanden bär på potential att väsentligt försämra Sinchs intäkter, lönsamhet och värdering. Enligt vår uppfattning underskattar marknaden dessa risker avsevärt. Vi noterar att Sinch inte har kommunicerat riskerna eller de senaste regulatoriska ingripandena mot företaget till investerare.

Investerare bör noggrant väga den betydande nedsidan som Sinchs exponering mot bluffsamtalssystemet innebär mot eventuella upplevda tillväxtmöjligheter.