Case Study: Google-Salesforce Third-Party Data Breach

By Cirra Published August 13, 2025 30 min read

Google–Salesforce Data Breach: A Comprehensive Analysis

Background: Google, Salesforce, and Their Integration

Google is one of the world's largest technology companies, known for its internet search, cloud services, and advertising platforms. **Salesforce**, by contrast, is the leading cloud-based Customer Relationship Management (CRM) provider, whose platform is used by businesses to manage sales leads, customer data, and marketing. The two companies have a long-standing partnership: since 2017, Salesforce and Google have integrated their products to help mutual customers connect sales, marketing, and advertising data (Source: salesforce.com)(Source: salesforce.com). In fact, Google itself has been a Salesforce customer – using Salesforce's CRM to engage with its own clients (Source: salesforce.com).

One such integration is Google's use of Salesforce to manage outreach to prospective Google Ads customers (primarily small and medium businesses) (Source: salesforceben.com). This means certain Google business data (like sales contacts and notes) reside in Salesforce's cloud environment, bridging the two companies' systems.

Nature of the Integration: In practical terms, Google's sales teams leverage Salesforce's CRM platform to track and communicate with business customers for services like Google Ads. Salesforce's platform can also be connected to Google's advertising and productivity tools. For example, Salesforce is integrated with **Google Ads** (to import lead conversion data) and **Google Analytics** (to connect online customer insights with CRM data) (Source: salesforce.com). The Salesforce-Google partnership includes deep connectivity between Salesforce's Sales/Marketing Cloud and Google Workspace (Gmail, Drive, etc.) (Source: salesforce.com)(Source: salesforce.com). Thus, Google's and Salesforce's systems are intertwined both as technology partners and as vendor-client: Google entrusts some of its corporate data to Salesforce's cloud, and Salesforce in turn uses Google Cloud infrastructure for some services (Source: salesforce.com)(Source: salesforce.com). This close integration set the stage for the **Google–Salesforce data breach**, in which attackers exploited the Salesforce side of Google's data management.

Timeline of Events

1. **March 2025:** Salesforce issued guidance warning customers of **rising social engineering attacks** targeting Salesforce users. They noted cases of voice phishing ("vishing") where attackers impersonate IT support to trick employees into adding malicious **connected apps** to Salesforce (Source: salesforce.com)(Source: salesforce.com). (Connected apps are third-party or external applications authorized to interface with a Salesforce org.)

2. **Early June 2025:** Google's Threat Intelligence Group (GTIG) published research on a vishing-based campaign by a threat actor it dubbed **UNC6040**, which was **targeting Salesforce customers** for large-scale data theft (Source: securityweek.com)(Source: cloud.google.com). GTIG identified that attackers were impersonating IT staff over the phone to persuade victims to install a fake Salesforce **Data Loader** application (a tool for bulk data export) (Source: cxtoday.com). No Salesforce software vulnerability was involved – instead, the attackers exploited human trust and Salesforce's extensibility features (Source: cxtoday.com)(Source: cloud.google.com). Google's June report linked these tactics to the notorious hacking group **ShinyHunters** and possibly **Scattered Spider**, known for past breaches (Source: securityweek.com)(Source: securityweek.com).

3. **June 2025 (same timeframe):** Unbeknownst to the public at the time, **Google itself fell victim** to the very attack GTIG had described. In an incident in mid-June, one of Google's corporate Salesforce instances (used for prospective Ads customer data) was breached via the UNC6040 vishing scheme (Source: bleepingcomputer.com)(Source: salesforceben.com). Attackers tricked a Google employee

into authorizing a malicious app, which allowed them to access and extract data from Google's Salesforce database. Google later noted it *"took swift action to remove the malicious app and cut off access as soon as we became aware"*(Source: woodslaw.com)(Source: woodslaw.com). At this stage, the breach was contained internally and not yet public.

4. **July 2025:** The campaign continued to unfold. On **July 16, 2025**, for example, **Allianz Life** (a U.S. insurance company) had a similar breach – an intruder used social engineering to access Allianz's third-party CRM (Salesforce) and steal customer data (Source: securityaffairs.com)(Source: securityaffairs.com). Allianz confirmed the incident at the end of July and notified law enforcement (FBI) (Source: securityaffairs.com). Throughout July, other major organizations – including airlines, retailers, and luxury brands – were attacked in this wave. Many began internal investigations and quiet notifications. (Notably, **Adidas, Qantas, Allianz, Cisco, Louis Vuitton, Dior, Tiffany & Co.** were later identified as victims of the same campaign (Source: bleepingcomputer.com).)

5. **Early August 2025:** The breach became public on a broad scale. On **August 5, 2025**, Google updated its June GTIG blog post to reveal **it was among the victims** of UNC6040 (Source: cloud.google.com). Google acknowledged that its Salesforce instance had been compromised in June and that data was stolen during a brief window before access was cut off (Source: bleepingcomputer.com)(Source: bleepingcomputer.com). Over the next few days (first week of August), **media reports** by cybersecurity outlets (e.g. BleepingComputer, SecurityWeek) and mainstream tech press began detailing the **"Google–Salesforce data breach"** and the larger campaign (Source: bleepingcomputer.com)(Source: securityweek.com). The threat actors, identifying themselves as **ShinyHunters**, claimed to have breached numerous companies' Salesforce databases and hinted at targeting at least one "trillion-dollar company" (suspected to be Google) (Source: bleepingcomputer.com)(Source: bleepingcomputer.com).

6. **August 8, 2025:** Google's GTIG stated it had completed emailing **notifications to all affected customers** whose information was in the compromised database (Source: cxtoday.com). Google emphasized that the stolen data was limited and largely not sensitive (more details below). The same week, companies like **Chanel** and **Pandora Jewelry** also disclosed they were impacted by the Salesforce-related breach, as threat actors began extortion attempts or public disclosure (Source: salesforceben.com)(Source: securityweek.com).

7. **August 11, 2025:** In response to Google's confirmation (and the cascade of victim disclosures), **Salesforce publicly addressed the issue**. Salesforce published a security advisory and a status update clarifying that **Salesforce's platform was not itself breached** – the incidents were due to *"sophisticated phishing and social engineering attacks"* against its customers (Source: securityweek.com). Salesforce urged all customers to strengthen their security settings, enable

multi-factor authentication, and audit connected apps (Source: salesforceben.com)(Source: salesforceben.com). The company reiterated that no Salesforce product vulnerability was exploited (Source: salesforceben.com).

8. **Mid August 2025:** The attackers escalated pressure. ShinyHunters (and affiliates) launched a leak site and Telegram channel to **publish stolen data** from victims who refused to pay ransom (Source: cloud.google.com)(Source: securityaffairs.com). By August 13, for instance, hackers **leaked 2.8 million records** from Allianz Life's Salesforce data – including customers' personal details and even tax IDs (Source: securityaffairs.com). This public dump confirmed the attackers' threat to expose data. Meanwhile, cybersecurity experts and law enforcement continued investigations. Reports also emerged that some victims quietly **paid ransoms** (one company paid ~$400,000 in Bitcoin) to prevent data leaks (Source: bleepingcomputer.com)(Source: woodslaw.com). The threat group boasted that even "**trillionaires like Google can't stop us**" and warned that future campaigns *"will be much, much worse"*(Source: salesforceben.com)(Source: salesforceben.com) – highlighting the brazen confidence of the attackers.

(Timeline Note: This campaign is ongoing. As of August 2025, more companies may yet discover breaches since some intrusions occurred months prior but only resulted in extortion now (Source: salesforceben.com). The timeline above focuses on key events around the Google-related breach and its immediate aftermath.)

How the Breach Occurred: Attack Vector and Technical Details

Attack Method – Voice Phishing (Vishing): The breach did not arise from a software flaw in Google or Salesforce systems, but from **social engineering**. The attackers used **phone calls** to impersonate IT support personnel and targeted employees who had access to their company's Salesforce CRM (Source: cxtoday.com)(Source: malwarebytes.com). This voice-phishing tactic, known as **vishing**, exploited human trust. By calling and pretending to be legitimate tech support, the attackers convinced victims that urgent action was needed on the Salesforce system.

Malicious "Data Loader" App: The specific ploy involved **tricking administrators into installing or authorizing a fake application** within Salesforce. In Google's case and others, the hackers guided an employee over the phone to install a purported Salesforce utility named something like "My Ticket Portal" – which was actually a **malicious version of Salesforce's Data Loader tool**(Source: cxtoday.com). (The real **Salesforce Data Loader** is a trusted tool used to bulk import/export data in a Salesforce database (Source: cxtoday.com). Because it has powerful data access privileges, it was an attractive target for abuse.) The fake application was introduced as a **connected app** in the Salesforce org, often by directing the user to Salesforce's app integration page and providing an **8-digit code** to connect to what the victim

thought was a legitimate tool (Source: malwarebytes.com)(Source: malwarebytes.com). Once the user entered the supplied code, they unknowingly granted the attackers' app **OAuth access** to the Salesforce instance.

Abusing OAuth and Connected Apps: By getting the victim to authorize the malicious app, the attackers obtained a valid session token and API access to the Salesforce data – effectively **bypassing normal login or multi-factor challenges** because an authenticated app was now approved (Source: cxtoday.com)(Source: cloud.google.com). The GTIG analysis noted that the fake Data Loader reused OAuth credentials and did not trigger obvious security alerts since it appeared as an authorized tool (Source: cxtoday.com). In essence, the criminals **exploited a feature** – the ability to add third-party connected applications to a Salesforce org – and turned it into a backdoor. Salesforce's own advisory confirmed this method, warning that attackers lured users to *"login.salesforce[.]com/setup/connect"* to add a malicious connected app, often a **modified Data Loader published under a misleading name**(Source: salesforce.com)(Source: salesforce.com).

Data Access and Exfiltration: Once the malicious app was connected, the attackers had **API access** inside the Salesforce environment with the permissions of the victim's account. They could quietly query, **extract, and download large sets of data** – exactly what Data Loader is designed to do (Source: cxtoday.com)(Source: cloud.google.com). The attackers likely automated this process. Google's Threat Intelligence team observed that the group initially used the Data Loader GUI, but later even switched to **custom Python scripts** to extract data via the Salesforce API, making the process faster and harder to trace (Source: cloud.google.com). The exfiltration traffic was routed through anonymity networks (like TOR or VPNs) to mask the source (Source: cloud.google.com). In Google's case, the unauthorized data access occurred within a *"small window of time"* before Google's security team detected and cut off the app's access (Source: bleepingcomputer.com). This suggests Google's monitoring caught the anomaly relatively quickly, limiting the exposure.

No Salesforce Platform Vulnerability: Importantly, **no inherent vulnerability in Salesforce's software was exploited** in these attacks. Both Google and Salesforce have stressed that the breach was made possible by *"exploiting trust and familiarity"*, not by hacking the code of Salesforce (Source: cxtoday.com)(Source: salesforceben.com). The attackers **manipulated an authorized user** to let them in through an official feature (connected apps). This means traditional technical defenses (firewalls, patches, etc.) were not the weak point – the human element was. As one expert summarized: *"This isn't a Salesforce vulnerability – it's a human-centric breach"*(Source: cxtoday.com).

Affected Systems: The primary system affected was **Google's Salesforce CRM instance** – a cloud database separate from Google's internal infrastructure. Google confirmed that only this Salesforce cloud environment was accessed; **no other Google systems or products were breached**(Source: salesforceben.com). In other words, the attackers did **not** reach Google's corporate network, user accounts, or Google Cloud systems – the damage was confined to the data within Salesforce. (Other

companies victimized similarly saw their Salesforce data compromised, but not necessarily their broader IT systems.) There are reports that in some cases the attackers attempted to pivot further – for example, using info from Salesforce to target Office 365 accounts of the same company (Source: malwarebytes.com) – but Google states it observed no such spread in its incident (Source: salesforceben.com).

To summarize, the breach of the Google-Salesforce data was achieved through **a clever blend of social engineering and abuse of Salesforce's integration capabilities**. The attackers **exploited trust**: trust of employees in supposed IT helpers, and trust of the Salesforce platform in connected applications. This allowed them to gain high-level access without cracking any password or breaking any firewall – essentially, they were **invited in by a misled user**.

Data Compromised: Types and Scope of Information Exposed

Google's Stolen Data: The targeted Salesforce database at Google contained **contact and sales information for SMB (Small/Medium Business) clients** of Google's ads division. According to Google's analysis, the data taken was *"confined to basic and largely publicly available business information"* – specifically **company names, contact names, phone numbers, email addresses, and related notes**(Source: bleepingcomputer.com)(Source: bleepingcomputer.com). No sensitive personal financial data, passwords, or Google account data were in that Salesforce instance. In effect, the breach exposed a B2B contact list and some internal notes about those business customers. Google has not publicly confirmed the exact number of records, but the ShinyHunters group claimed to have stolen approximately **2.55 million records** from the Google database (Source: cxtoday.com). It's worth noting that these were mainly business contacts; much of it could be considered "directory information" that might already be on business websites or public listings (Source: cxtoday.com)(Source: cxtoday.com). Google's statement reinforced that point to downplay severity, but it was still a theft of proprietary data.

Data from Other Companies: The broader campaign compromised many firms' Salesforce data, and the sensitivity of information varied by victim. For example, Allianz Life's breach was far more **sensitive**: the hackers obtained **2.8 million records** including individuals' full names, addresses, dates of birth, and tax identification numbers, as well as details on financial advisors and policies (Source: securityaffairs.com). That is highly confidential personal data. In other cases (Adidas, Qantas, Chanel, etc.), the stolen data reportedly included customer contact info and marketing data – such as email addresses, loyalty program details, or sales histories (Source: salesforceben.com). **Reports suggest that the majority of breached data across victims was personal contact information and corporate client data (names, emails, phone numbers, company names)**, and **not** things like passwords or credit card numbers (Source:

salesforceben.com). There has not been evidence of financial account data or sensitive intellectual property being stolen via these Salesforce attacks as of mid-August 2025 (Source: salesforceben.com) (Source: salesforceben.com).

Scope of the Google Breach: Within Google's incident specifically, the scope was limited to one Salesforce **"org"** (instance) used by a particular business group. Google clarified that the affected records were related to *"prospective Ads customers"*(Source: salesforceben.com). Thus, current Google Ads customers' billing or account info was not in this dataset, and no Google user accounts were exposed. The breach did **not** involve consumer data like Gmail accounts or search history – it was purely a corporate CRM database. **All affected business customers (whose contact info was taken)** have been notified by Google via email (Source: cxtoday.com). Because the data was mostly business contact info, many data privacy laws (which focus on personal consumer data) may not have been triggered – a fact that has its own implications (discussed below in Legal/Regulatory consequences).

In summary, the data compromised in the Google-Salesforce breach was **sales contact data for millions of small businesses**. While arguably "low sensitivity" compared to passwords or credit card numbers, this information can still be **abused by threat actors**. It provides a ready-made list of targets for **phishing or fraud** (since it identifies who the key contacts are at various companies) (Source: woodslaw.com). Internal notes and context could be used to craft convincing scam emails. Additionally, for other companies in this campaign, significant personal data was exposed, raising the stakes beyond just business contacts.

Public Statements and Responses from Google and Salesforce

Google's Response: Google formally disclosed the breach through an update to its Threat Intelligence blog and statements to the press in early August 2025. In its public remarks, Google acknowledged the incident and provided reassurance on the limited impact. A Google spokesperson stated that the event *"affected a limited set of data in one of Google's corporate Salesforce instances used to communicate with prospective Ads customers"*(Source: salesforceben.com). They emphasized that the **compromised data was basic business contact info** and that Google's security teams had **contained the issue and put mitigations in place immediately**(Source: salesforceben.com). Google stressed that **no Google internal systems or products were accessed** and there was *"no impact to data contained in Google products or Google Cloud"*(Source: salesforceben.com). In other words, the breach was isolated to the Salesforce-hosted database.

Google also took on the task of notification and transparency. By August 8, the Google Threat Intelligence Group reported it had **completed email notifications** to all customers or individuals whose information was stolen (Source: cxtoday.com). These notices likely went to the small business contacts in the database, informing them that their work contact details had been exposed. Google's Threat Intelligence

blog promised further updates if new information emerged and shared indicators of compromise to help others defend against the threat (Source: cloud.google.com)(Source: cloud.google.com). Internally, Google's security incident response kicked in promptly in June when the breach was detected – they removed the malicious app and cut off the attacker's access quickly (Source: woodslaw.com). Google has not indicated it will offer any credit monitoring (since no highly sensitive personal data was taken), but it has used the incident to raise awareness of this kind of supply-chain/social engineering threat.

Salesforce's Response: Salesforce, as the CRM provider involved, responded by clarifying the nature of the incident and guiding customers on security best practices. In an advisory posted on its **Trust Status** page and echoed in public statements, Salesforce asserted that **its platform was not compromised** – *"The Salesforce platform has not been compromised, and this issue is not due to any known vulnerability in our technology"*(Source: salesforceben.com). Salesforce positioned the breaches as a result of *"phishing threats [that] continue to rise"* and reaffirmed its commitment to supporting affected customers (Source: salesforceben.com)(Source: salesforceben.com).

Salesforce's message to all customers was to **strengthen their security posture** in light of these attacks. They pointed users to a company blog post on key platform security features and **best practices**(Source: salesforceben.com). Specifically, Salesforce urged administrators to **enable multi-factor authentication (MFA)**, enforce **least privilege access controls**, and **carefully manage connected apps** in their Salesforce orgs (Source: salesforceben.com)(Source: salesforce.com). They also recommended reviewing who can create or install new connected apps and to remove or restrict any unused integrations (Source: salesforceben.com). In essence, Salesforce's response was to educate and remind that security is a "shared responsibility" – the provider can offer tools, but customers must use them properly to protect their data (Source: salesforce.com)(Source: salesforce.com). Salesforce's Security team had anticipated these tactics earlier in the year (as seen in their March 2025 blog), so their public response reinforced measures they'd already been advocating.

One notable aspect of Salesforce's handling is the **reputational angle**: The company took care to distance the **brand "Salesforce"** from the word "breach" by emphasizing it wasn't their cloud hacked. As one commentary put it, Salesforce found itself like a landlord whose tenants left the doors unlocked – it wasn't Salesforce's tech failing, but it's still their name in the headlines (Source: salesforceben.com) (Source: salesforceben.com). Salesforce pledged to "fully support" customers and encouraged any with security questions to contact support for help (Source: salesforceben.com). There was no admission of any liability on Salesforce's part (indeed, technically none of their systems were broken into), but a clear effort to **guide customers and protect trust** in the platform.

In addition to Google and Salesforce, some of the other victim companies also made public statements: for example, Allianz Life filed official breach notices and stated it had contained the incident and involved law enforcement (Source: securityaffairs.com). Companies like **Pandora** and **Chanel** quietly confirmed

their incidents to the media without extensive detail, given the data was similar types of contact info. The uniform theme was that each company saw only their **Salesforce-hosted data** hit, and their core networks remained secure. All indicated they were enhancing security and assisting any affected clients.

Reactions from Security Researchers and Experts

The infosec community reacted to the Google-Salesforce breach with a mix of alarm and "lessons learned" commentary. Many experts noted the **irony** that Google's own Threat Intelligence team had *warned* about the very tactics that ended up compromising Google. As Salesforce Ben put it, this was *"one of the most high-profile instances yet of a security team publicly warning about a threat actor's tactics, only to be successfully targeted by them."*(Source: salesforceben.com). This twist underscores that **even the best-resourced organizations are not immune** to social engineering. *"If it can happen to Google, it can happen to anyone,"* observed cybersecurity writers (Source: cxtoday.com).

Several security researchers highlighted that the attack was **not technically sophisticated** – it relied on deception – but that adversaries are augmenting age-old cons with modern tools. For instance, the ShinyHunters group claimed to be using **AI-generated voices** during vishing calls to make them more convincing and evade identification (Source: salesforceben.com)(Source: salesforceben.com). By using AI voices, the attackers can spoof different identities and even defeat attempts to trace calls (no background noise or identifiable vocal patterns) (Source: salesforceben.com). This development worried experts, as it shows how **advances in AI can empower social engineering**. Law enforcement officials, including possibly the NSA, are reportedly struggling to trace these vishers since traditional voice recognition and call tracing techniques fall short against AI-masked voices (Source: salesforceben.com).

From a defense perspective, experts like those at Huntress and others pointed to several takeaways. **Dray Agha**, a Senior Security Operations manager at Huntress, noted in Forbes that anytime you use third-party cloud vendors, you *"must rigorously vet and continuously monitor all vendors with access to your data."*(Source: cxtoday.com). In this case, Google's use of Salesforce (a third-party) expanded their attack surface – a risk that had to be managed continuously. The breach highlights the importance of **vendor risk management** and ensuring partners meet high security standards. However, it also showed that even a secure platform can be misused if humans are tricked.

Security professionals also strongly recommended **security awareness training** in light of these events (Source: cxtoday.com). The success of the vishing scam underscores that employees are the last line of defense. Regular training on how to spot phishing/vishing, how to verify callers (e.g., calling back via official company numbers), and how to handle unusual IT requests could prevent such incidents. As one analyst observed, these social engineering attacks were "not especially sophisticated" in a technical sense, but they exploit basic human trust – something that technology alone can't fix (Source: cxtoday.com).

Another reaction concerned the **time-delay and persistence** of this campaign. Google GTIG and others found that the extortion (data leaks or ransom demands) often occurred **months after the initial breach**(Source: cloud.google.com)(Source: cloud.google.com). This suggests attackers quietly sit on stolen data, possibly even selling access to others (one theory being UNC6040 stole data and UNC6240 handled extortion as a "second stage") (Source: securityweek.com). Some researchers suspect multiple threat groups (ShinyHunters, Scattered Spider, and even Lapsus$ members) may be collaborating, given the techniques and the bragging on hacker forums (Source: securityweek.com)(Source: securityaffairs.com). In fact, in mid-August the attackers formed a Telegram channel combining aliases ("ScatteredSpiderHunters") to publicize their successes (Source: securityaffairs.com). This cross-group collaboration is a concerning trend noted by experts – it could lead to more **aggressive attacks and public data dumps** as criminals join forces.

Notably, **law enforcement** has been involved in investigating this string of breaches. The FBI was notified in at least one case (Allianz) (Source: securityaffairs.com). There have been arrests of some individuals tied to the broader groups in the past year (Source: securityweek.com), but the core operators of this campaign remain at large. Security experts caution that as long as such attacks remain lucrative (with some victims paying large ransoms), they will continue. The attackers' own statements – taunting that "billionaires are nothing" to them and claiming law enforcement will forget about them in a month – reflect a bold confidence and likely indicate they will lay low and strike again later (Source: salesforceben.com)(Source: salesforceben.com). Researchers are using the indicators from this campaign (phishing email addresses, VPN exit nodes, etc.) to help companies detect and block similar attempts (Source: cloud.google.com)(Source: cloud.google.com), but consensus in the community is that **vishing and app-based CRM attacks may increase** after this high-profile success.

In summary, the expert reaction coalesces around a few points: (1) **No one is immune** – even top tech firms can be breached via social engineering. (2) **Fundamentals matter** – training, vendor vetting, least privilege, and monitoring could have mitigated or prevented these attacks. (3) Attackers are innovating on the social front (using AI, multi-stage schemes), so defenders must up their game accordingly. The breach has become a case study in the cybersecurity community about the importance of human-centric security measures in the era of cloud SaaS services.

Legal, Regulatory, and Reputational Consequences

Legal and Regulatory Fallout: The Google–Salesforce breach and the connected attacks on other companies have prompted legal scrutiny and the need for compliance with data breach laws. Since Google's stolen data involved business contact information rather than consumer personal data, the **legal requirements for notification** were somewhat murky. In many jurisdictions, breach notification laws (like state data breach statutes or GDPR in Europe) focus on personal identifiable information of individuals.

Google did proceed with voluntary notifications to affected businesses (Source: cxtoday.com), but as one analysis pointed out, **many breach laws don't strictly compel notification for B2B data**(Source: woodslaw.com)(Source: woodslaw.com). This has raised concerns that some victims whose data was stolen (e.g. small businesses in the Google Ads prospect list) might never be formally notified by their business provider due to loopholes in breach laws (Source: woodslaw.com)(Source: woodslaw.com). In Google's case, they did notify, but not every company might have if the data wasn't legally defined as personal data.

For companies like Allianz Life and others where personal customer data was exposed (names, contact info, birth dates, etc.), breach notification laws do apply. Allianz, for example, disclosed the breach through the Maine Attorney General's office, indicating compliance with U.S. state laws requiring notification when certain personal data is compromised (Source: securityaffairs.com). Regulatory bodies such as state Attorneys General and European Data Protection Authorities are likely monitoring these incidents. If any European residents' data was involved, Google and others might also have to report under GDPR's 72-hour notification rule to EU regulators. So far, no regulatory fines or enforcement actions have been publicly announced, but investigations could be underway given the high profile of the victims.

Law Enforcement: As mentioned, the FBI was contacted in at least one case (Allianz) (Source: securityaffairs.com). International law enforcement cooperation may be involved since the threat actors are targeting companies globally (Adidas in Europe, Qantas in Australia, etc.). The global and extortionate nature of the crime (demanding Bitcoin ransoms) puts it in the realm of serious cybercrime cases that agencies like the FBI, Interpol, etc., would pursue. However, these investigations take time and the attackers' use of anonymization and AI voice spoofing makes it challenging. Over the past year, **some members of ShinyHunters and affiliated groups were arrested**(Source: securityweek.com), but it's unclear if those arrests have impeded this particular campaign. The attackers' brazen communications suggest they remain active and confident, at least for now (Source: salesforceben.com).

Potential Lawsuits: In the wake of the breach, at least one U.S. law firm (Woods Lonergan) announced it is **investigating a possible class-action lawsuit** related to the Google Salesforce CRM breach (Source: woodslaw.com)(Source: woodslaw.com). They are seeking to represent businesses whose data may have been compromised. Such a lawsuit would likely argue that Google (and/or Salesforce) **failed to adequately protect the data** or promptly inform affected parties (Source: woodslaw.com)(Source: woodslaw.com). Possible claims could include negligence in cybersecurity practices or breach of contract/confidentiality for not safeguarding clients' information (Source: woodslaw.com). The law firm's outline suggests they may invoke laws like state data protection acts (e.g., New York's SHIELD Act) and even FTC Act provisions on unfair practices (Source: woodslaw.com)(Source: woodslaw.com). It remains

to be seen if these legal actions gain traction, given the data involved is business data. Nevertheless, it shows that **companies like Google could face civil liability** if clients argue that proprietary data (like sales leads) was a valuable asset compromised by lax security.

Salesforce might also face legal claims indirectly – though Salesforce wasn't breached, an argument might be made (fairly or not) that Salesforce should have done more to prevent abuse of its connected app system. Indeed, another law firm announced an investigation targeting Salesforce and the impacted companies (Source: lynchcarpenter.com). If multiple customers of Salesforce suffer breaches due to similar tactics, there could be pressure on Salesforce regarding the security of its ecosystem. At minimum, Salesforce will be keen to avoid any perception of legal responsibility by continuously stating it has provided security features and the issue was misuse.

Reputational Impact on Google: For Google, the breach is a bruise to its reputation as a security leader. While the data lost was not highly sensitive, the fact that Google – with its formidable security resources – got tricked by a phone scam drew some surprise and criticism (Source: cxtoday.com). It was a headline-grabbing story that one of the world's most powerful tech companies fell victim to a basic social engineering hack (Source: cxtoday.com)(Source: cxtoday.com). In the cybersecurity community, this incident humbles even the big players, but in the public/business community, it could cause some embarrassment. That said, because the breach was limited in scope, Google likely won't suffer long-term damage to user trust in its core products (no consumer passwords or usage data were exposed). Google handled disclosure responsibly and aligned with best practice, which helps mitigate reputational harm. Moreover, Google can frame this as an example of *"we're all human, mistakes happen"* and use it to champion better security awareness training industry-wide.

Reputational Impact on Salesforce: Salesforce faces a tricky reputational issue. Technically, its security was not beaten – but its name is all over these breaches since they happened *through* Salesforce instances. Companies and their customers might grow uneasy: *"Is my data safe in Salesforce cloud?"* Salesforce has been doing damage control by emphasizing the platform's security and shifting focus to how clients use it (Source: salesforceben.com). The scenario is reminiscent of a cloud provider whose customer misconfigures something – it's not the cloud's fault, but it's still problematic. Salesforce's stock or customer confidence could take a short-term hit, especially among less tech-savvy clients who see the word "Salesforce" and "data breach" together in news. Long-term, Salesforce will need to ensure its **trust messaging** is loud and clear and possibly introduce even more guardrails (like improved monitoring for suspicious connected apps on their end). So far, Salesforce has navigated it by being proactive in guidance and asserting no breach on their side, which is crucial to preserving their trusted image.

Broader Consequences: This incident is likely to have industry-wide effects. Regulators and industry groups may push for stronger security requirements for SaaS applications and third-party integrations. Enterprises might re-evaluate their **third-party risk management** – for example, doing more rigorous security reviews of how they use SaaS like Salesforce and what data they store there. Cyber insurance

implications also arise: insurers will take note of this campaign and may update policy terms or premiums related to social engineering and vendor breaches. We might also see calls for clearer legal standards on B2B data protection. As the law firm analysis pointed out, currently **"most federal and state data breach laws do not require companies like Google to notify affected businesses"** when business data is stolen (Source: woodslaw.com). There could be a push to close that gap so that businesses are alerted when their data held by a vendor is breached, even if it's not personal consumer data.

In summary, the legal/regulatory aftermath is still unfolding. Google and its fellow victims have thus far complied with notification practices and involve law enforcement. The **reputational hit** is real but contained: it serves as a cautionary tale more than a scandal. Ultimately, the incident's biggest consequence may be a wake-up call and catalyst for improved security measures across the tech industry, which leads into the final section on lessons learned.

Lessons Learned and Best Practices for Prevention

The Google-Salesforce breach highlights several **critical lessons** for organizations to protect against similar incidents. Here are the key takeaways and best practices, distilled for a cybersecurity-savvy audience:

- **Vigilant Security Awareness Training:** Technical defenses mean little if employees are duped into opening the door. Companies must invest in regular, comprehensive **security awareness training** focusing on phishing and **vishing** recognition (Source: cxtoday.com). Staff should be trained to verify any unsolicited "IT support" calls – for example, by independently contacting their real IT department. In this case, an administrator instructed to install unfamiliar software could have paused and checked with security, which would have stopped the attack. Simulated phishing/vishing exercises can be useful to keep employees alert. In an era of AI-driven voice scams, training should include the possibility that a caller may not be who they claim, even if the voice sounds convincing.

- **Strict Control of Third-Party Apps and Integrations:** Businesses using cloud platforms like Salesforce should **audit and lock down their connected applications**. **No user should be able to install or authorize a new integration without oversight**(Source: salesforceben.com). Administrators should maintain an allow-list of approved apps and block all others by default (Source: salesforce.com). Regularly review the list of connected apps in your CRM – remove any that are unused or unknown. Salesforce Ben (a community site) strongly urged admins to *"identify the origin of all connected apps, remove unused/unknown apps, and remove the ability for any user to add connected apps without approval."*(Source: salesforceben.com). Had Google's team done this, the employee would not have been able to add the fake "My Ticket" app without higher-level sign-off. In Salesforce specifically, one can restrict who has the "Manage Connected Apps" or "Modify All Data" permissions (Source: salesforce.com) – this should be limited to as few people as possible.

- **Principle of Least Privilege:** Apply **least privilege** rigorously to accounts and data access. The more privileges a user has, the more damage if they are compromised. In CRM contexts, limit which accounts can export large data sets or create API tokens (Source: salesforce.com)(Source: salesforce.com). For example, not every sales user needs the ability to use Data Loader or run massive reports. In Google's case, perhaps a lower-tier account without admin rights would not have been able to install an app or pull millions of records. By limiting privileges (and segmenting data so one account can't see it all), you contain the blast radius of any single account being phished.

- **Multi-Factor Authentication (MFA) Everywhere:** Ensure MFA is enabled on all accounts, especially for access to critical systems like Salesforce (Source: salesforceben.com)(Source: salesforce.com). While in this campaign the attackers bypassed login by using OAuth tokens, MFA still provides an important layer (for instance, if they had tried to steal credentials outright, MFA could stop them). Also, consider using **FIDO2 security keys or number-matching MFA prompts** for higher assurance. Beyond just user logins, some platforms allow MFA for application access or API calls; if available, use it. At the very least, MFA will thwart many less sophisticated attacks and force adversaries to resort to social engineering like this – which you then address with the other measures.

- **Network and Access Restrictions:** Implement network-based access controls for cloud admin interfaces. Salesforce allows setting **trusted IP ranges** for login (Source: salesforce.com). If possible, restrict administrative access to VPN or corporate IPs, so an external bad actor calling an employee can't simultaneously log in from a foreign IP without triggering alerts or being blocked. In this campaign, the attackers used TOR/VPNs to access Salesforce (Source: cloud.google.com); if the target companies had IP whitelisting, those login attempts might have been prevented or flagged immediately.

- **Monitor for Anomalous Activity:** Use logging and monitoring tools to detect unusual data access patterns. Salesforce provides **event monitoring** (part of Salesforce Shield) that can alert on mass data downloads or new app installations (Source: salesforce.com)(Source: salesforce.com). Companies should ensure such monitoring is active, and alerts are sent to security teams in real time. In Google's scenario, they did catch the intrusion quickly – likely due to monitoring that saw a spike in data export activity. Every organization should similarly monitor their CRM for large exports, especially of contacts, or sudden creation of objects like connected apps. Set up **thresholds** (e.g., alert if > X records are exported within Y minutes) and investigate immediately. Having a SIEM (Security Information and Event Management) ingest these logs can facilitate detection of a breach in progress.

- **Incident Response Planning:** *"It's not if but when,"* as the saying goes (Source: cxtoday.com). Businesses must have a well-tested **incident response plan** for data breaches. The plan should include steps for quickly revoking compromised credentials or apps, analyzing impacted data,

preserving logs, and notifying stakeholders. Google's swift containment shows the value of having practiced IR procedures. An Incident Response Plan ensures that even if an attacker slips through, the damage can be minimized and handled in an orderly way. Table-top exercises involving a scenario of a SaaS breach would be very beneficial after this event.

- **Vendor Risk Management:** Treat your **SaaS providers and cloud vendors as extensions of your environment**, and secure them accordingly. Regularly review the security features of third-party platforms (like Salesforce's security tools) and make sure you're leveraging them fully. Also, ensure that vendors have their own strong security – in this case Salesforce did, but the integration point was the weakness. When onboarding any third-party service that will hold your data, ask about features like audit logs, admin controls, and support in case of a security incident. As Dray Agha noted, continuous monitoring of vendors is key (Source: cxtoday.com). For instance, if Salesforce (or any critical vendor) issues a security advisory, treat it with urgency and implement recommendations promptly.

- **Enhanced Verification of Unusual Requests:** Introduce policies that any request to install software or make significant system changes undergo secondary verification. This could be an internal policy where the employee must get approval from InfoSec for such changes, or even a technical enforcement (as noted with connected app restrictions). Additionally, establish a way for employees to easily confirm if a person contacting them is legitimate. For example, if "IT support" calls about Salesforce, your staff should know to hang up and call the official IT helpdesk. This kind of two-factor verification for instructions can derail vishing. Encourage a culture where employees won't be reprimanded for double-checking identities – **better safe than sorry**.

In conclusion, the Google-Salesforce breach serves as a stark reminder that **cybersecurity is a shared responsibility**(Source: salesforce.com). Cloud providers must supply secure platforms and robust security features (which Salesforce does), and customers must configure and use those features correctly while keeping their people educated. By combining technical controls (like MFA, IP restrictions, least privilege) with human-focused defenses (training, verification policies) and having an incident plan, organizations can **dramatically lower the risk** of falling prey to similar attacks (Source: salesforce.com) (Source: cxtoday.com). The incident's ultimate lesson is that even in a time of advanced technology, fundamental security practices and vigilance are indispensable. As businesses implement these best practices, they strengthen their defenses so that a voice on the phone or a cleverly disguised app will not so easily become their undoing.

Sources:

- Google Threat Intelligence Group – *"The Cost of a Call: From Voice Phishing to Data Extortion"* (Official Google Cloud Blog) (Source: cloud.google.com)(Source: cloud.google.com)

- BleepingComputer – *"Google suffers data breach in ongoing Salesforce data theft attacks"* (Lawrence Abrams, Aug 6, 2025) (Source: bleepingcomputer.com)(Source: bleepingcomputer.com)
- Salesforce Ben – *"Salesforce Forced to Issue Data Theft Warning as Google Confirms It Is Among Victims"* (Thomas Morgan, Aug 11, 2025) (Source: salesforceben.com)(Source: salesforceben.com)
- CX Today – *"The Google-Salesforce Customer Data Breach: What Really Happened?"* (Rhys Fisher, Aug 12, 2025) (Source: cxtoday.com)(Source: cxtoday.com)
- Malwarebytes Labs – *"How Google, Adidas, and more were breached in a Salesforce scam"* (David Ruiz, Aug 7, 2025) (Source: malwarebytes.com)(Source: malwarebytes.com)
- SecurityWeek – *"Google Discloses Data Breach via Salesforce Hack"* (Eduard Kovacs, Aug 6, 2025) (Source: securityweek.com)(Source: securityweek.com)
- SecurityAffairs – *"Hackers leak 2.8M sensitive records from Allianz Life in Salesforce data breach"* (Pierluigi Paganini, Aug 13, 2025) (Source: securityaffairs.com)(Source: securityaffairs.com)
- Woods Lonergan PLLC – *"Google Salesforce CRM Data Breach"* (Legal analysis for class action, Aug 2025) (Source: woodslaw.com)(Source: woodslaw.com)

Tags: data breach, cybersecurity, third-party risk, cloud security, salesforce, crm security, data privacy

---

About Cirra

About Cirra AI

Cirra AI is a specialist software company dedicated to reinventing Salesforce administration and delivery through autonomous, domain-specific AI agents. From its headquarters in the heart of Silicon Valley, the team has built the **Cirra Change Agent** platform—an intelligent copilot that plans, executes, and documents multi-step Salesforce configuration tasks from a single plain-language prompt. The product combines a large-language-model reasoning core with deep Salesforce-metadata intelligence, giving revenue-operations and consulting teams the ability to implement high-impact changes in minutes instead of days while maintaining full governance and audit trails.

Cirra AI's mission is to **"let humans focus on design and strategy while software handles the clicks."** To achieve that, the company develops a family of agentic services that slot into every phase of the change-management lifecycle:

- **Requirements capture & solution design** – a conversational assistant that translates business requirements into technically valid design blueprints.

- **Automated configuration & deployment** – the Change Agent executes the blueprint across sandboxes and production, generating test data and rollback plans along the way.
- **Continuous compliance & optimisation** – built-in scanners surface unused fields, mis-configured sharing models, and technical-debt hot-spots, with one-click remediation suggestions.
- **Partner enablement programme** – a lightweight SDK and revenue-share model that lets Salesforce SIs embed Cirra agents inside their own delivery toolchains.

This agent-driven approach addresses three chronic pain points in the Salesforce ecosystem: (1) the high cost of manual administration, (2) the backlog created by scarce expert capacity, and (3) the operational risk of unscripted, undocumented changes. Early adopter studies show time-on-task reductions of 70-90 percent for routine configuration work and a measurable drop in post-deployment defects.

Leadership

Cirra AI was co-founded in 2024 by **Jelle van Geuns**, a Dutch-born engineer, serial entrepreneur, and 10-year Salesforce-ecosystem veteran. Before Cirra, Jelle bootstrapped **Decisions on Demand**, an AppExchange ISV whose rules-based lead-routing engine is used by multiple Fortune 500 companies. Under his stewardship the firm reached seven-figure ARR without external funding, demonstrating a knack for pairing deep technical innovation with pragmatic go-to-market execution.

Jelle began his career at ILOG (later IBM), where he managed global solution-delivery teams and honed his expertise in enterprise optimisation and AI-driven decisioning. He holds an M.Sc. in Computer Science from Delft University of Technology and has lectured widely on low-code automation, AI safety, and DevOps for SaaS platforms. A frequent podcast guest and conference speaker, he is recognised for advocating "human-in-the-loop autonomy"—the principle that AI should accelerate experts, not replace them.

Why Cirra AI matters

- **Deep vertical focus** – Unlike horizontal GPT plug-ins, Cirra's models are fine-tuned on billions of anonymised metadata relationships and declarative patterns unique to Salesforce. The result is context-aware guidance that respects org-specific constraints, naming conventions, and compliance rules out-of-the-box.
- **Enterprise-grade architecture** – The platform is built on a zero-trust design, with isolated execution sandboxes, encrypted transient memory, and SOC 2-compliant audit logging—a critical requirement for regulated industries adopting generative AI.
- **Partner-centric ecosystem** – Consulting firms leverage Cirra to scale senior architect expertise across junior delivery teams, unlocking new fixed-fee service lines without increasing headcount.
- **Road-map acceleration** – By eliminating up to 80 percent of clickwork, customers can redirect scarce admin capacity toward strategic initiatives such as Revenue Cloud migrations, CPQ refactors, or data-model rationalisation.

Future outlook

Cirra AI continues to expand its agent portfolio with domain packs for Industries Cloud, Flow Orchestration, and MuleSoft automation, while an open API (beta) will let ISVs invoke the same reasoning engine inside custom UX extensions. Strategic partnerships with leading SIs, tooling vendors, and academic AI-safety labs position the

company to become the de-facto orchestration layer for safe, large-scale change management across the Salesforce universe. By combining rigorous engineering, relentlessly customer-centric design, and a clear ethical stance on AI governance, Cirra AI is charting a pragmatic path toward an autonomous yet accountable future for enterprise SaaS operations.
