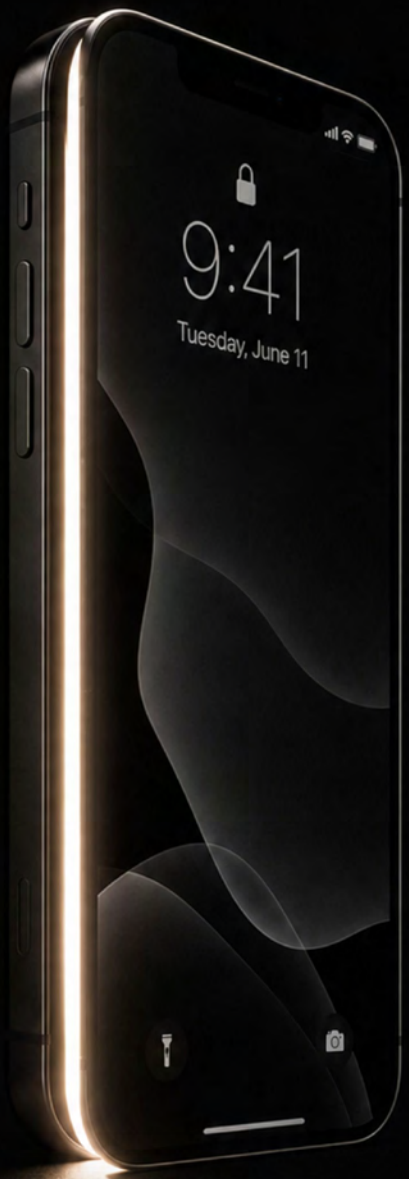
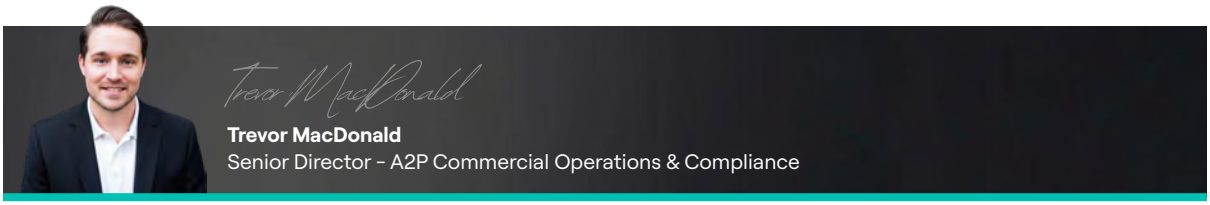
syniverse®



Spam Doesn’t Knock on Just One Door

How unwanted messages reach your phone even when everything is set up right, and what Syniverse is doing about it.



A Quick Note Before We Start

If you work anywhere near messaging, you have heard these two common assumptions: "If I got a spam text, someone must have been hacked," and "If spam reached my customer, it came through their aggregator." I want to be upfront, both are usually wrong, and believing them sends people chasing a problem that isn't there.

Here is the truth this paper is built around: a phone is not one door, it is a hallway full of them. We have built strong controls around business messaging. They work, but they only govern some of those doors. Spam reaches people by walking through the others.

What follows is how that happens. We'll cover the channels and tricks bad actors use to get around the systems meant to stop them, real examples we see, and the work our teams do to fight it, and to help the industry get smarter about it. It is written to be shared, with our own teams and with customers.

– Trevor

Contents

The Misconception

Two beliefs come up again and again and both are comfortable because they let everyone off the hook. The first is that spam means someone got hacked. The second is that if a spam message reached a customer, it must have ridden in through the aggregator that carries their legitimate traffic.

Here's an example of spam that I received. I was waiting on a delivery, a gift for my wife, and I knew the shipper would text me when it was out for delivery so I could grab it off the porch before someone walked off with it. Yes, a little paranoid. Right on cue, a text showed up saying the package was held and I needed to click a link to reschedule. I was annoyed enough that I almost tapped it. Then I looked closer. It had come in over Rich Communication Services (RCS) on the person-to-person path, not from the shipper's real number, and the link looked off. So instead of clicking, I logged into my account on the shipper's site directly, where the package was still right on track. Then I copied the link into a URL scanner and ran it through Browserling, a sandboxed browser, to be safe. Both flagged it as spam.

That is the problem in one message. I was expecting a legitimate text on a normal channel, and a scam walked straight into that expectation through a door the shipper never used.

Most of the time, neither is true. No system was breached, and the message did not come in on a registered campaign. The spam took a completely different road to the phone, one that was never built to check who is sending or what they are sending.

That distinction matters. If we tell a customer "you must have been hacked" or "your provider let it through," we send them chasing the wrong problem. The honest answer is harder and more useful: a modern phone has many separate entry points, and the controls we have put around business messaging only govern some of them.

The Many Doors Into Your Phone

Every channel is a way in. Spam can arrive on any of them, even the registered, monitored ones.

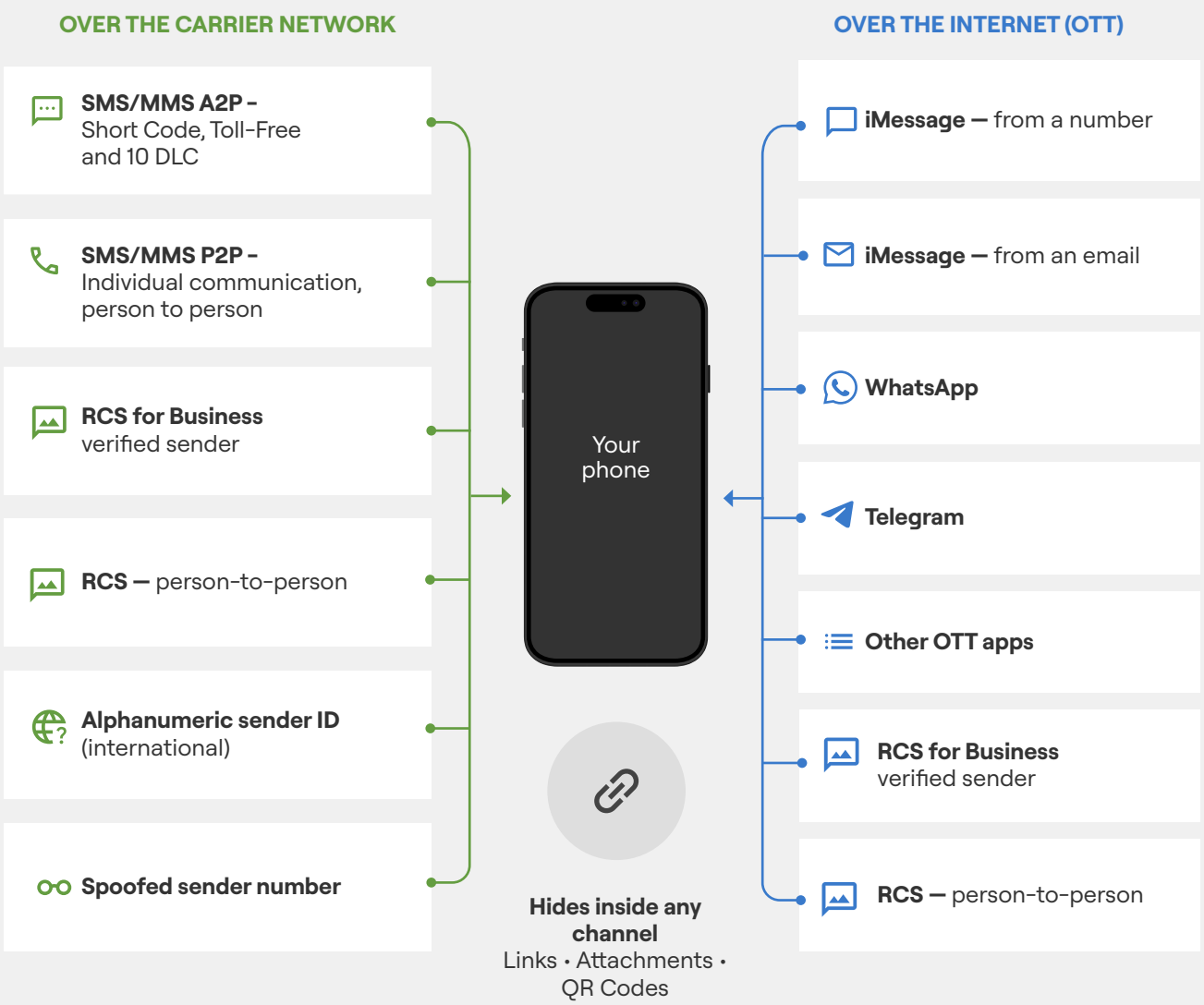


Figure 1. Every channel is a separate way in. Spam can arrive on any of them, including the registered, monitored paths.

How A2P Messaging Gets Registered and Why That Matters

Let me start with what does work, because it is the reason bad actors bother with workarounds at all.

Legitimate application-to-person (A2P) messaging, the texts from your bank, your pharmacy, your airline, registers before it can send. In the United States there are three main registered paths. 10-Digit Long Code (10DLC), toll free, and short code traffic are registered and verified before messages flow.

This is not just a U.S. story. Many countries run their own sender-ID registries and industry bodies operate a Sender ID Protection Registry that lets brands register the names they send under so impostors can be blocked. Even some of the over-the-top (OTT) apps, the messaging apps that run over the internet rather than the carrier network, have their own business registration and verification programs.

The common thread is simple. Legitimate business messaging is increasingly identifying itself, getting vetted, and being monitored. That is exactly why spam does not usually try to come through the registered front door. It goes around it.

What is Governed — and How Bad Actors Get Around it

Legitimate business messaging registers itself and is monitored, Abuse takes the paths that were never built to check.

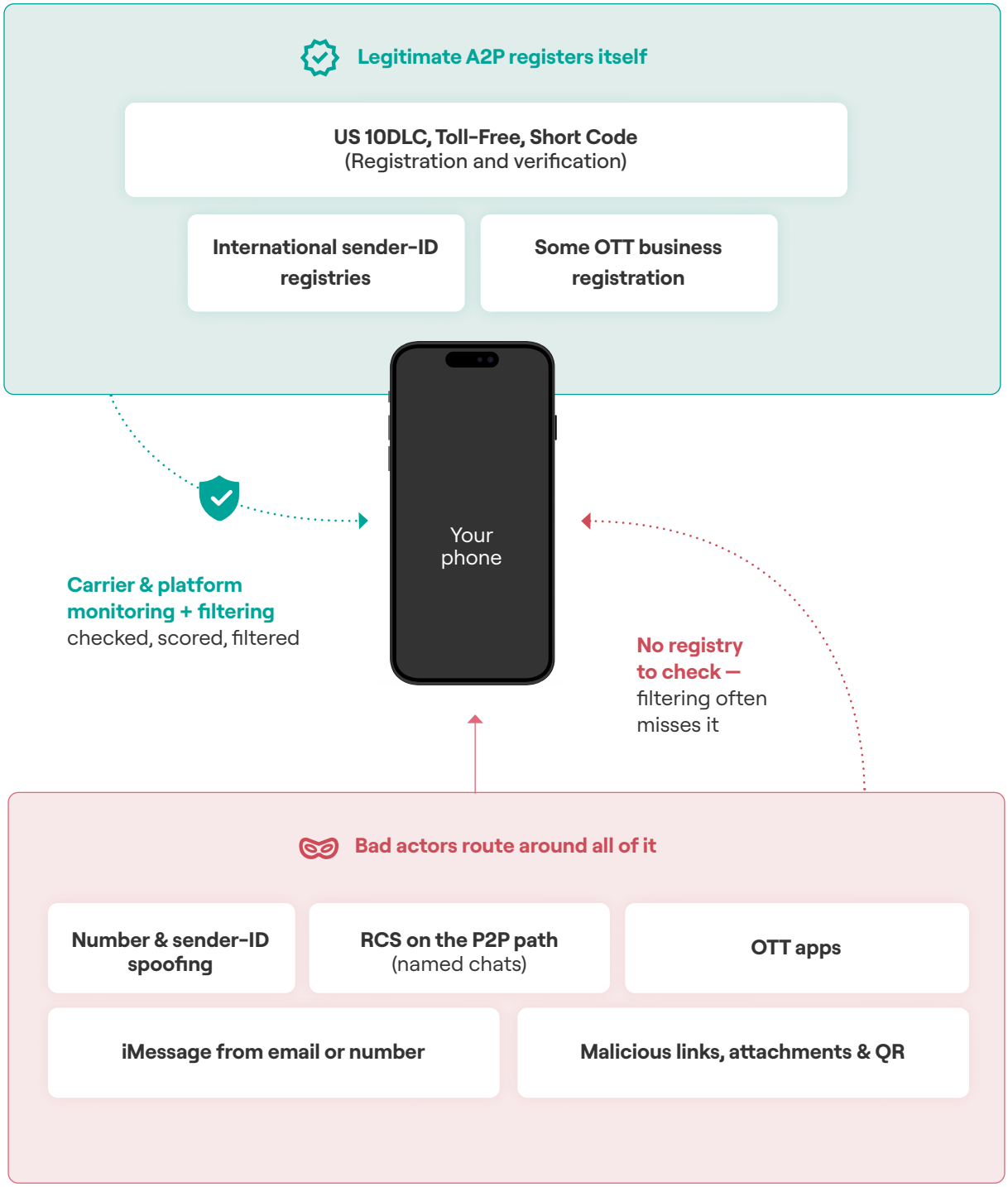


Figure 2. Registered traffic identifies itself and is monitored. Abuse takes the paths that were never built to check.

The Doors the Registry Doesn't Guard

Here is where the misconception breaks down. Registration governs the front door. It does nothing for the side doors, and there are a lot of side doors.

Spoofed numbers

A phone number shown as the sender is not proof of who actually sent the message. Sender information on SMS can be faked, so a text can appear to come from a local number, a bank's line, or a government office while originating somewhere else entirely. The number you see is a label, not a guarantee.

Alphanumeric sender IDs, internationally

In much of the world, businesses send SMS using an alphanumeric sender ID, a short name like "MyBank" instead of a number. In countries that do not run a sender-ID registry, there is often nothing stopping a bad actor from setting that same name and impersonating the brand. The message lands looking exactly like the real thing.

RCS on the P2P path

RCS is the richer successor to SMS, and for verified businesses it shows a branded, check marked sender. But RCS also has a person-to-person (P2P) path, and on that path someone can create a chat and give it a business-sounding name. To the person receiving it, an unverified P2P chat can look a lot like a legitimate business, and as RCS adoption grows, this is a tactic worth watching.

iMessage, from a number or an email

iMessage rides over the internet, and that gives bad actors two openings. They can send from a regular phone number that appears as iMessage, including international numbers far from where the message claims to originate, and they can send from an email address. When a "job offer" or an "Apple security alert" arrives as iMessage from a random Gmail or Outlook address, that is the tell.

OTT apps: WhatsApp, Telegram, and others

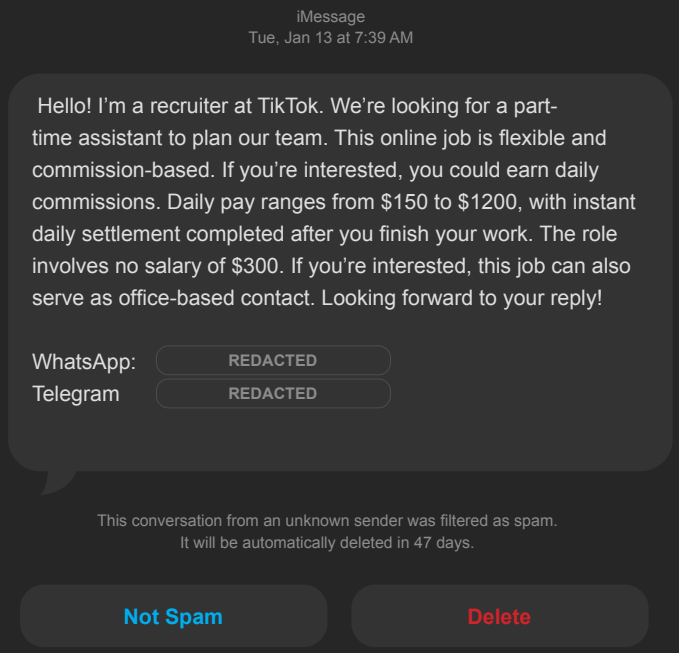
OTT apps sit entirely outside the carrier network, so carrier and aggregator controls simply do not apply to them. This is now one of the largest spam surfaces there is. Researchers analyzing years of scam reports found that the majority of malicious links in these messages had never even been analyzed by security services, let alone blocked. The platforms are fighting back. Meta reported removing nearly seven million WhatsApp accounts tied to scam activity in a single crackdown, but the volume tells you how big the problem is. The "Hi Mum" family-impersonation scam alone has cost victims millions.

Links, attachments, and QR codes

Finally, the payload often is not text at all. A link, a PDF attachment, or a QR code can ride inside almost any channel and carry the victim off the phone entirely, to a fake payment page or a credential-harvesting site. A QR code is especially sneaky, because it hides the destination until the camera opens it.

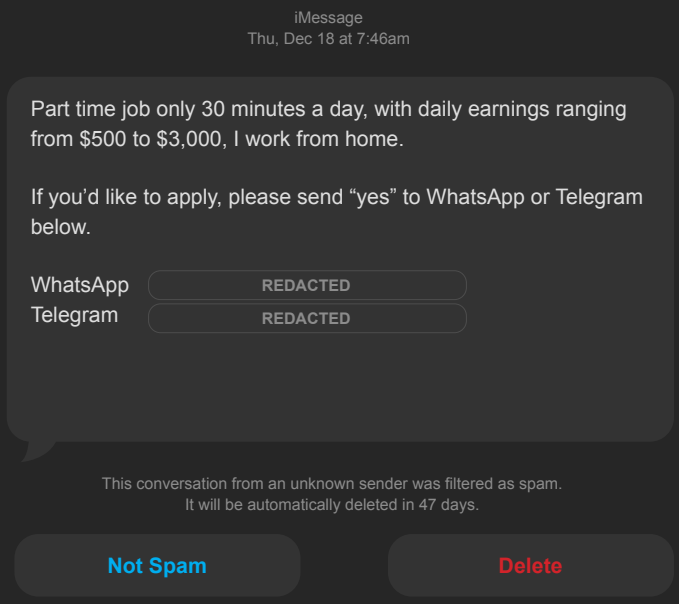
Real Examples We See

These are real messages, lightly cleaned up. We have removed the sender IDs, and we have blocked out the live scammer phone numbers, links, and QR codes so this document is safe to share. What we kept is the part that teaches: the channel it came in on, and the trick it used.



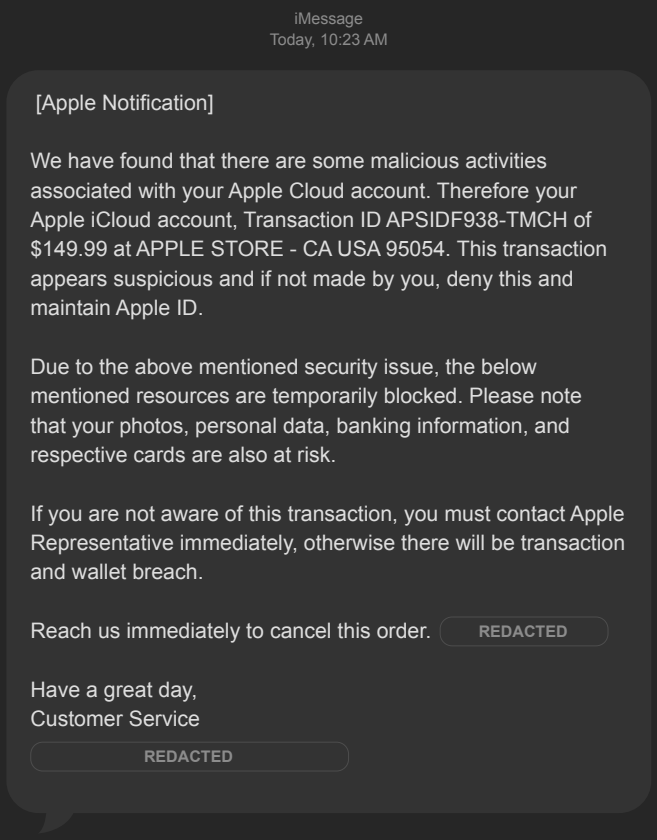
1

iMessage, from an email address. A fake TikTok "recruiter" job that pushes you to WhatsApp or Telegram. Apple already flagged it as spam.



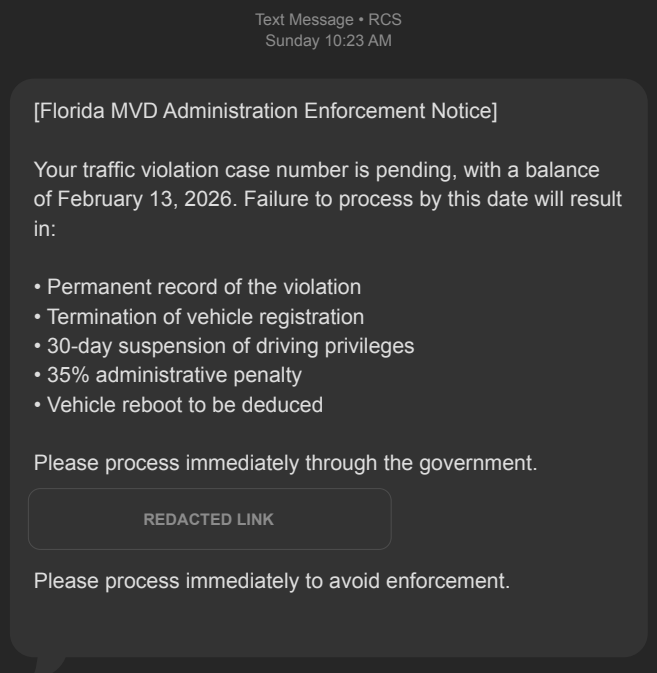
2

iMessage, from an email address. A "task" job scam promising big daily pay, again steering you to OTT apps.



3

iMessage, from an email address. A fake Apple security alert. A real Apple notice does not arrive from an Outlook address.



4

RCS. A fake Florida DMV "enforcement notice" with a redacted phishing link and heavy false urgency.

iMessage
Tue, Jan 13 at 7:39 AM

Maryland Motor Vehicle Administration
Your license/permit will take effect on March 31.

According to our records, you have an outstanding fee and/or remedial process requirement.

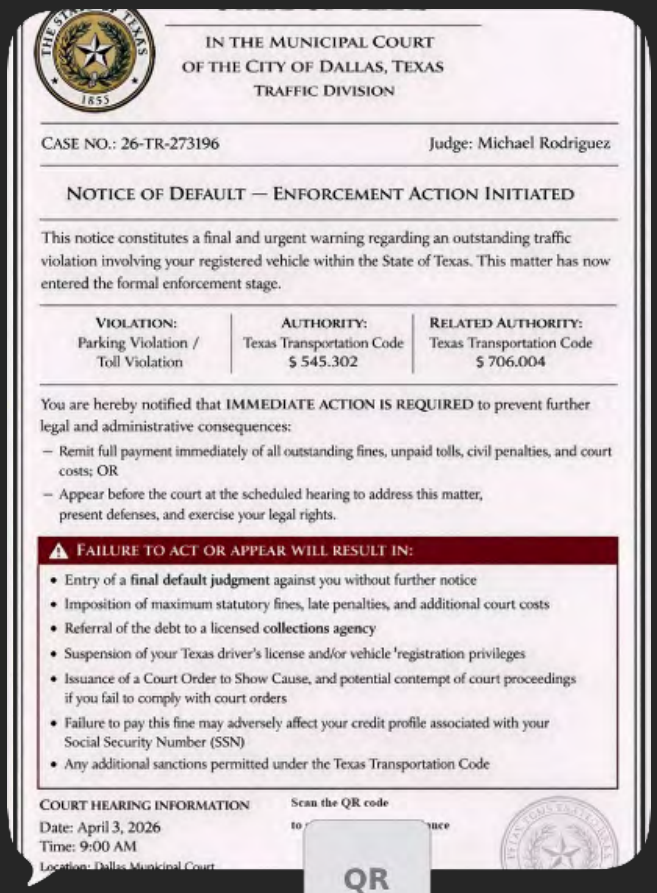
Per Maryland regulation 16C-16-004, failure to complete required by March 30, 2020 may result in:

1. Entry of the violation into official records
2. Suspension of vehicle

5

iMessage, from an international number. A fake Maryland MVA traffic-ticket notice.

Text Message • SMS
Tue, Jan 13 at 7:39 AM



IN THE MUNICIPAL COURT
OF THE CITY OF DALLAS, TEXAS
TRAFFIC DIVISION

CASE NO.: 26-TR-273196 Judge: Michael Rodriguez

NOTICE OF DEFAULT — ENFORCEMENT ACTION INITIATED

This notice constitutes a final and urgent warning regarding an outstanding traffic violation involving your registered vehicle within the State of Texas. This matter has now entered the formal enforcement stage.

VIOLATION:	AUTHORITY:	RELATED AUTHORITY:
Parking Violation / Toll Violation	Texas Transportation Code § 545.302	Texas Transportation Code § 706.004

You are hereby notified that IMMEDIATE ACTION IS REQUIRED to prevent further legal and administrative consequences:

- Remit full payment immediately of all outstanding fines, unpaid tolls, civil penalties, and court costs; OR
- Appear before the court at the scheduled hearing to address this matter, present defenses, and exercise your legal rights.

⚠ FAILURE TO ACT OR APPEAR WILL RESULT IN:

- Entry of a **final default judgment** against you without further notice
- Imposition of maximum statutory fines, late penalties, and additional court costs
- Referral of the debt to a licensed **collections agency**
- Suspension of your Texas driver's license and/or vehicle registration privileges
- Issuance of a Court Order to Show Cause, and potential contempt of court proceedings if you fail to comply with court orders
- Failure to pay this fine may adversely affect your credit profile associated with your Social Security Number (SSN)
- Any additional sanctions permitted under the Texas Transportation Code

COURT HEARING INFORMATION
Date: April 3, 2026
Time: 9:00 AM
Location: Dallas Municipal Court

Scan the QR code

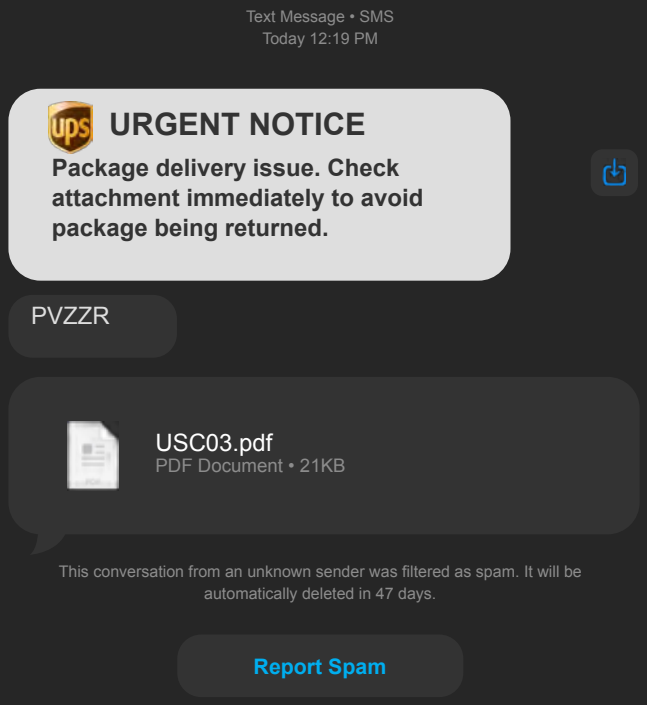
QR

This conversation from an unkno ered as spam. It will be automatically ys.

Report Spam

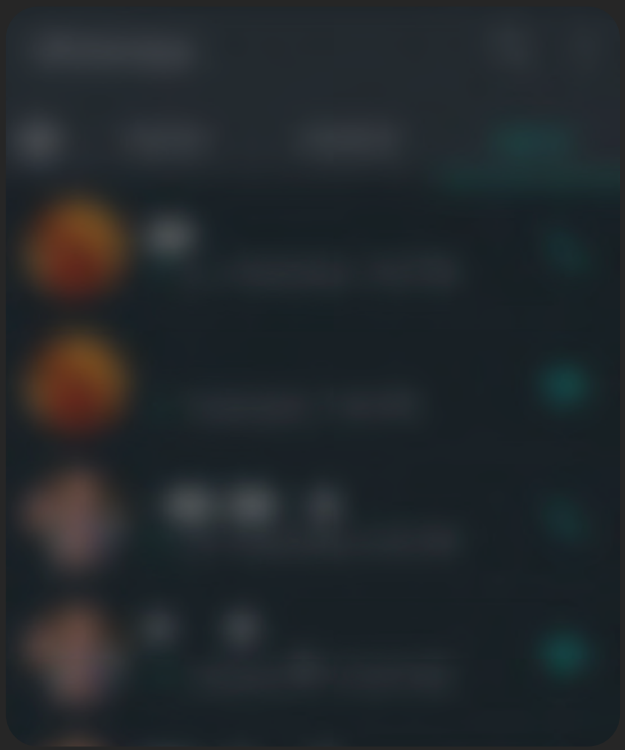
6

SMS. A fake Texas court "notice of default" carrying a redacted QR code to a payment page.



7

SMS, with a PDF attachment. A fake UPS delivery alert that wants you to open the file.



8

WhatsApp / OTT
Shown as a channel, not content. We collect OTT examples too, but several involve people in genuine distress, so we describe them rather than display them.

The Same Picture, By Channel

Different doors, same goal. Notice the last column: almost none of these are governed by A2P registration, because the message never used the registered path.

Channel	How it reached the phone	Common trick	Governed by A2P registration?
SMS, alphanumeric (intl)	A brand name set as the sender	Bank and brand impersonation	Only where a sender-ID registry exists.
RCS, P2P path	A chat named like a business	Looks verified but is not	No. P2P is not registered A2P.
iMessage	Over the internet, by number or email	Job and security alert scams	No. It is outside carrier A2P.
OTT (WhatsApp, Telegram)	Over the internet, app to app	Investment, "Hi Mum," job scams	No. It is outside the carrier network.
Links, attachments, QR	Ride inside any channel	Malware, fake payment pages	No. The payload is not the sender.

Why This Matters

If you take one thing from this paper, take this: a phone is not one door, it is a hallway full of them. Registration and monitoring lock the doors we built and watch, and they do that job well. But a user has many other ways in, and a bad actor only needs one of them.

That is why "you got hacked" and "it came through your aggregator" are not just wrong, they are unhelpful. They point the customer at a door that was never opened. The real story is that the message walked in through a side door, and the more channels a person uses, the more doors there are.

What Syniverse is Doing About it

This is what we're proud of, we are not just describing the problem, we are working on it from several directions.

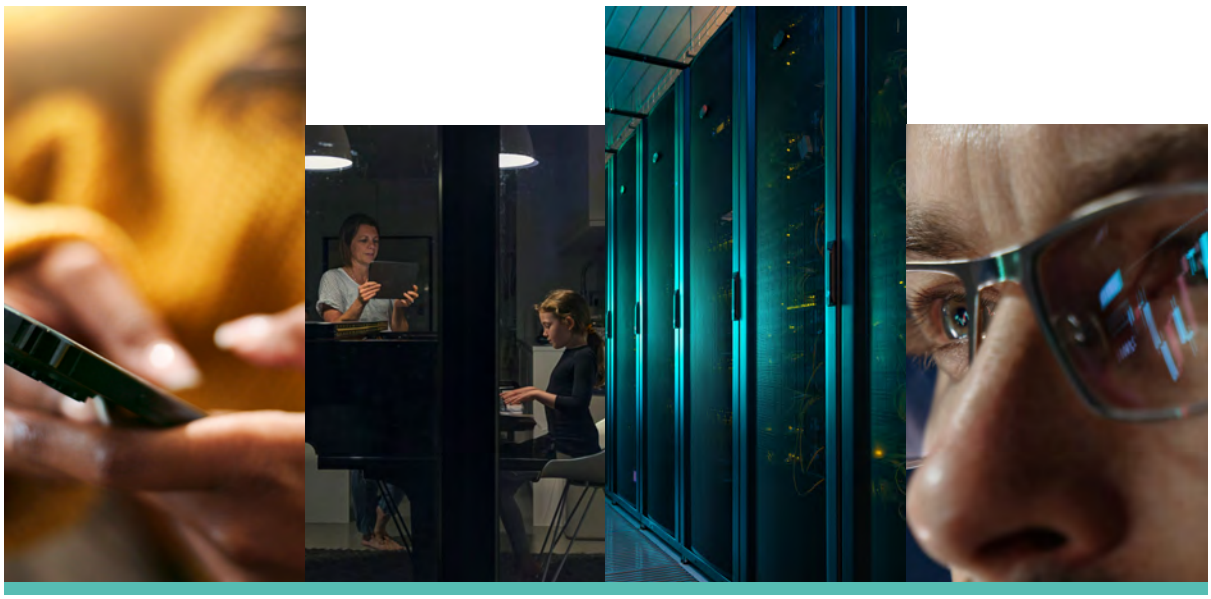
First: detection. Our Messaging Trust and data science teams run AI-assisted systems that look for spam and fraudulent traffic in the messages we carry, combining machine detection with human oversight. We share what we see back with our enterprise customers so it feeds their own risk and fraud processes. As a Direct Connect Aggregator with direct carrier relationships, we sit close to the network, which gives us a strong vantage point to spot abuse and act on it.

Second: identity. Spam and fraud both lean on pretending to be someone they are not, so we invest in verifying who is really there, with capabilities like phone number verification and SIM swap detection that help confirm a person or a sender is genuine.

Third: the industry work. A lot of the fight against spam happens in the rooms where the rules get written. Syniverse serves on the boards of the Cellular Telecommunications Industry Association (CTIA), the Mobile Ecosystem Forum, and Campaign Verify, the bodies shaping messaging integrity, sender-ID protection, and brand verification. And our own contribution to the 10DLC framework that cleaned up so much U.S. long-code abuse is backed by a U.S. utility patent. We help build the front doors, and then we help keep them honest.

Our work has been recognized externally. In 2026, Frost & Sullivan named Syniverse the recipient of its Global Competitive Strategy Leadership Award in enterprise messaging, pointing to our Messaging Trust operations and identity services as a reason messaging is becoming a fraud-mitigation layer, not just a transport channel. We don't lead with awards, but it is fair validation that the approach is working.

Fourth: education, which is why this paper exists. The more our teams and our customers understand that spam has many entry points, the better we all get at spotting it, advising on it, and not chasing the wrong cause.



A Hands-On Way to Learn: The Phishing Game

The best way to get good at spotting these messages is to practice. That is the idea behind a phishing game I have been building. It's a simple, hands-on way to train people to recognize the tells we have walked through here: the wrong sender address, the false urgency, the off-channel ask, the link or QR code that does not belong. It puts the lessons in this paper into your hands instead of just on the page. The patent is pending.

I'm happy to set up a walkthrough. Schedule a session today.

Closing

Spam will keep looking for the unlocked door. Our job is to keep closing the ones we can, keep watching the ones we can't, and make sure the people we serve know the difference. If this paper helps you have a clearer, more honest conversation with a customer about how a message really reached them, it did its job.

– Trevor

Trevor's bio

Trevor MacDonald is Senior Director - A2P Commercial Operations & Compliance at Syniverse and a leading voice shaping the future of enterprise messaging. With more than 20 years in the industry, including key roles at Verizon helping drive adoption of emerging technologies such as IoT and 5G — Trevor brings a rare blend of technical depth and go-to-market leadership to the evolving messaging ecosystem. He spearheads initiatives that accelerate growth, elevate customer experience, and unite cross-functional teams. As a trusted advisor, he provides strategic guidance on building scalable messaging programs and navigating complex regulatory landscapes. He holds both an MBA and a U.S. Utility Patent.

References:

1. Lu, Allison, Medeiros, Bernardo B.P., Butler, Kevin R.B., Traynor, Patrick. May 2026. An Analysis of Mobile Messaging Scams Using Reddit Data. ResearchGate. (SMS and OTT scam links largely unanalyzed and unblocked).
2. Meta | WhatsApp. August 2025. New WhatsApp Tools and Tips to Beat Messaging Scams. Reporting on the removal of nearly seven million WhatsApp accounts tied to scam activity.
3. Report Fraud / UK National Fraud Intelligence Bureau. 2023 – 2026. "Hi Mum/Dad" WhatsApp UK Impersonation Scam Reports.
4. Ecosystem Forum, SMS SenderID Protection Registry.
5. Frost & Sullivan. 2026. Syniverse: 2026 Global Enterprise Messaging Services Competitive Strategy Leadership Award.

syniverse®