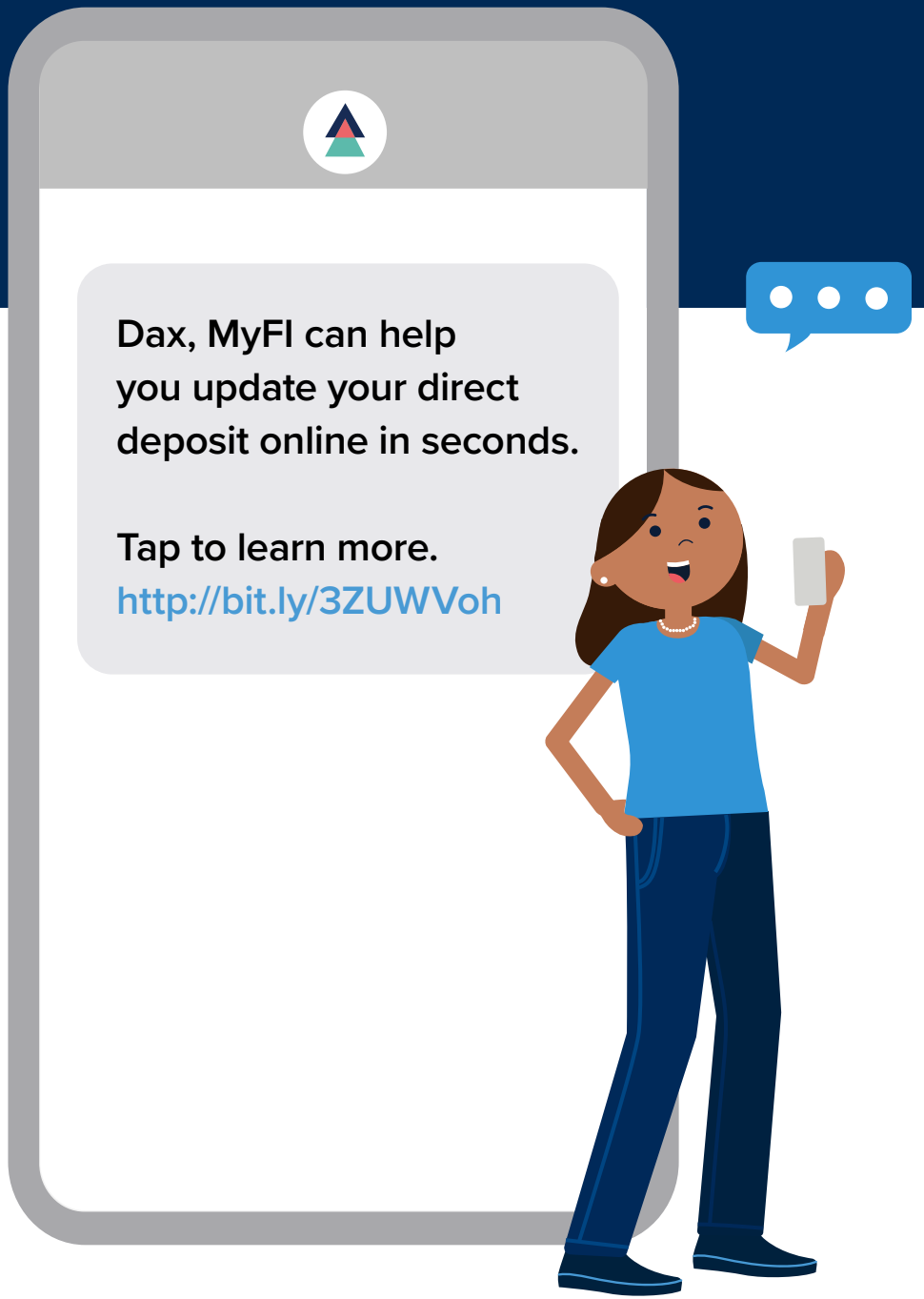
DIGITAL ONBOARDING

Text messaging: Manage the risks & reap the rewards

A guide for banks & CUs



Introduction

SMS text messaging provides your bank or credit union with a fast, convenient, and effective way to communicate with your customers and members. Some financial institutions are already using this channel to communicate—and seeing great results with it—while others either aren't using it yet or are just getting started.

If your bank or credit union isn't using text messaging yet, you should be. Consider this:

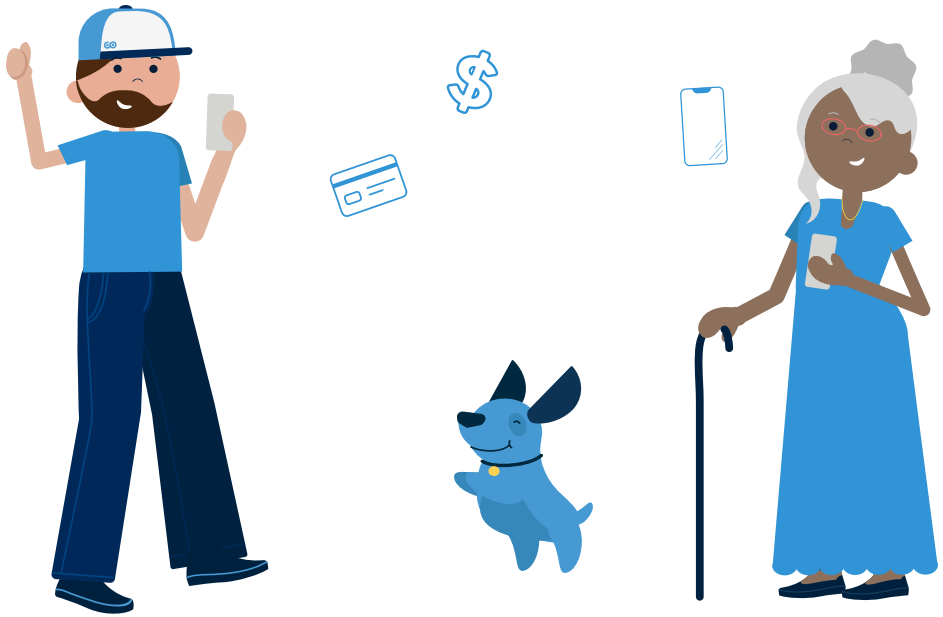
- Text messages are shorter (typically limited to fewer than 160 characters) and more personalized than other forms of communication.
- Americans check their phones on average 96 times per day and 95% of text messages are read within three minutes.
- According to Gartner, 98% of all text messages are opened, which is nearly five times higher than the average email open rate. And consumers respond to 45% of all text messages.
- Digital Onboarding's own platform has seen a 30% lift in click-through rates (CTRs) for text messaging compared to email.
- Nine out of 10 consumers prefer to communicate with businesses through text message, whether via alerts, reminders, or back-and-forth communication. This is especially true of younger generations.

> We saw an immediate positive response when we launched text messaging. We wanted to leverage this communication channel with our customers, and the opt-in widget gives us peace-of-mind that we are compliant with the process."

DUSTIN ATKINS
SVP, COO/CIO, PEOPLES BANK OF EAST TENNESSEE

Moreover, text messaging can help your bank or credit union:

- Maximize new account activation rates by providing immediate information to your customers and members about how to access and use their account.
- Increase cross-sell rates, as text messaging allows for more personalization when offering customers potential products.
- Keep people and businesses informed about time-sensitive events such as a system outage or branch closure.
- Grow customer and member satisfaction, as today's consumers have a strong preference for mobile banking and mobile communication.



> I don't think it's a debate of whether you (as a financial institution) should do texting. I have teenagers in my house. I don't think they know what email is. They don't do email. Texting is their preferred choice ... If you're not communicating via text, you're going to miss an audience. You have to be in that channel, but you also have to do it with an organizational-wide view."

MICHAEL THOMAS
SVP OF COMMUNICATIONS
GREATER NEVADA CREDIT UNION

Getting started with text messaging

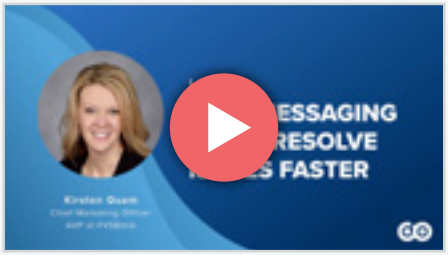
Using text messaging may seem like a big deal, but it isn't. Your bank or credit union has likely done something similar before, such as when you first started using email or social media channels like LinkedIn, Twitter, and Facebook to communicate. In other words, you just need to take what you already know and approach text messaging as you did other communication channels for the first time—by first making the business decision to use it and then asking and answering some high-level questions.

Questions to ask:

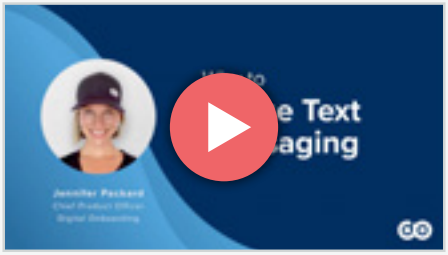
- What is the business purpose for using this communication channel?
- When and how will this channel be used to communicate with customers and members?
- Who at your company needs to be involved in launching and overseeing your text messaging efforts?
- What workstreams and processes need to be set up to support text messaging, and how will your company train employees on how to use it?
- What rules and policies will you establish for using it?

Here are some helpful videos on using text messaging:

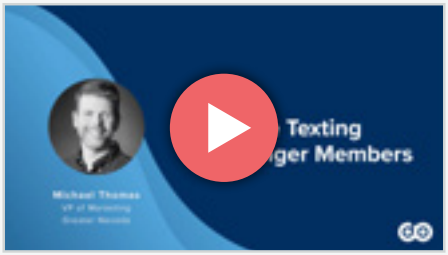
HOW TEXT MESSAGES HELP RESOLVE ISSUES FASTER



FINANCIAL INSTITUTIONS SHOULD UTILIZE TEXT MESSAGING



PRIORITIZE TEXTING FOR YOUNGER MEMBERS

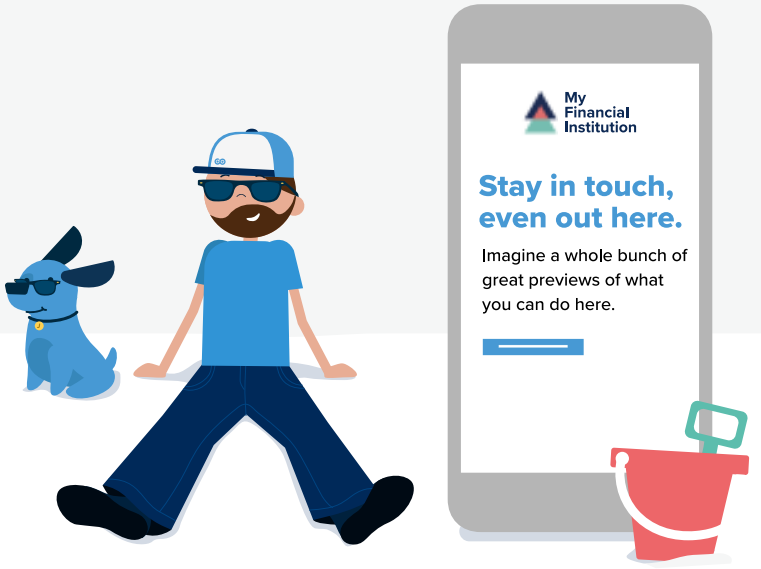


Your company should also:

- Understand how text messaging fits into your organization's broader operational plans in such areas as technology, security, fraud, and risk management.
- Identify and address the potential risks of text messaging to your organization. Text messaging is regulated by the Federal Communications Commission (FCC) under the Telephone Consumer Protection Act, so be sure to follow their guidelines carefully.
- Create a marketing plan that offers guidelines on how to successfully produce and implement your text message campaigns. Include an **internal checklist** in your plan of the steps your company needs to take to launch and support text messaging.

To help you create that checklist, review and answer the following questions:

- ☐ Which departments in your organization will be sending out SMS messages to customers and members?
- ☐ Should those departments be using the same code/number?
- ☐ Will any of those departments strictly be sending out transactional-type messages? (Define the reasoning so everyone internally is aware, as there are different regulations for customer transactional messages vs. educational and marketing messages, and there may be a different code required for transactional messages.)
- ☐ Do you prefer a dedicated short code vs. a shared short code? Or could a long code work just as well for your organization?
- ☐ Do you understand the compliance requirements of sending SMS to your customers?
- ☐ Do you have a way for people to easily opt-in and opt out of receiving SMS messages?
- ☐ Do you have a list of approved message types that you can send to customers?
- ☐ Do you also have a list of the types of text messages that everyone agrees will never be sent to customers?
- ☐ Has your compliance team approved all the above?
- ☐ What are your company's defined and approved steps that employees should take if a customer has a concern about a message they received or if a message is actually a security concern?
- ☐ Does your customer-facing staff have the training needed on the above to help guide a member or customer through the process and/or determine which text messages have been sent out by your company and which ones haven't?
- ☐ Have your customers been educated on the above?
- ☐ Does your company have a way of tracking that your employees have read and understand the above?



Best practices for using text messaging

As you begin texting with customers, it's important to keep these guidelines in mind:

Prior to launching text messaging

- Before sending any texts, collect opt-ins from the customers and members you plan to text. You need their permission before you reach out, and you must collect those opt-ins in a legally compliant way. Digital Onboarding's automated opt-in adoption platform offers an Email & SMS Text Opt-In Widget that makes this fast and easy.

> Education is key when you're launching something new...Just take a step back and say, 'What are the things we need to do to launch this and let's get the right people involved to do so.'"

JENNIFER PACKARD
CHIEF PRODUCT OFFICER
DIGITAL ONBOARDING

Sending text messages

- Use text messages in addition to email—not as a replacement. Sending consistent messages through multiple communication channels makes them more likely to be noticed and read.
- Send all text messages from a single, trusted phone number, such as from a five- or six-digit short code.
  - Short codes are used in one-way business-to-consumer messaging and aren't meant for personal, one-to-one messaging. Short code messages convey information to a customer that doesn't require a response but encourages them to take an action or simply provides them with important information.
  - There are two types of short codes: shared short codes and dedicated short codes. Your company can either find a vendor who can help you through the process of filing for approved short codes, or you can file for your own short codes and hope that the vendor you're using to send your messages accepts them.
  - Short codes are appealing for a few reasons:
    - They're pre-approved by carriers to avoid spam flags, giving them higher delivery rates than longer numbers.
    - They're easy for customers to remember and provide brand recognition and security.
    - Shared short codes are cost-effective for mass communication.
    - Shared short codes are also fast and easy to set up and have no setup fees.
- Include the name of your bank or credit union in every text message your company sends.
- Make sure any custom website URLs your company uses in text messaging look and feel safe. For instance, use *"https://www.yourbankname.com/webinar"* instead of something that looks questionable, such as *"http://www.b2+vmyUR/webinar??."* Shortened URLs are also beneficial, especially if your financial institution is sending out more than a few hundred text messages per day and you don't want those messages flagged as spam.
- Don't send too many messages. Only text your customers and members when your company needs to communicate timely or important information to them.

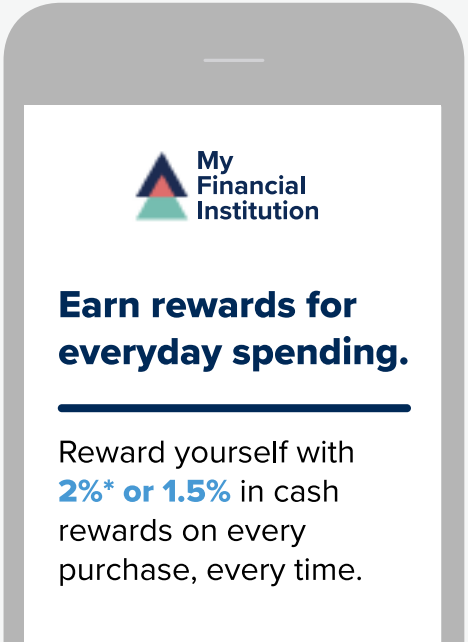
Customer education

- Proactively educate your customers and members about what type of information and text messages they can expect to receive from your company.
- Post your bank or credit union's privacy policy and text messaging guidelines on your company's website.

Organizational practices

- Start slowly when rolling out text messaging as a communication channel.
- Incorporate text messaging (e.g., reminders, alerts, and communication) into your bank or credit union's customer or member application and onboarding processes.
- Work with service providers that can help your organization incorporate all these best practices.

Besides using text messaging to communicate with customers and members, your bank or credit union can also use it to send marketing messages. Just make sure you're following the rules set forth in the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM).



The risks of text messaging

One of the biggest risks of using text messaging is that scammers and fraudsters also use it. The most common texting scam is called smishing, which is a type of cybersecurity attack that's similar to email phishing but is sent via text messages instead.

In this scam, cyber criminals create and send text messages that look like they come from legitimate businesses. But these messages contain false and misleading information that's designed to trick the recipient into disclosing personal information, such as their password, Social Security number, or credit card information. These messages may also include a URL or link to a fake website that prompts the receiver to download something onto their mobile device or computer that may seem legitimate but is actually harmful, such as a virus or ransomware. It's a multibillion-dollar business.

"Whether your bank or credit union uses text messaging or not, it's still likely to be the target of a smishing attack at some point."

SY PHUL
CHIEF INFORMATION SECURITY OFFICER
DIGITAL ONBOARDING

Unfortunately, because most people don't know what smishing is and don't recognize it when they see it, there's been a dramatic increase in smishing attacks over the past few years:

- The Federal Communications Commission recently reported that the number of smishing and scam text messages that target consumers nearly tripled from 2019 to 2022.
- Smishing attacks increased more than 700% in the first two quarters of 2021.
- In April 2022, an estimated 2,649,564,381 smishing messages were sent per week.

Some banks and credit unions mistakenly think the best way to protect themselves from a smishing attack is just to not use text messaging at all. But the reality is that many companies that don't use text messaging are still attacked. So, it's crucial to have a plan in place that addresses what your company will do if/when an attack happens.

> There are different ways cyber criminals can attack you, and it's a multi-layered attack when it's sophisticated enough."

SY PHUL
CHIEF INFORMATION SECURITY OFFICER
DIGITAL ONBOARDING

How to minimize the risks

There are a few key things you can do to protect your bank or credit union and its customers or members against the risks of a smishing attack:

Inform your customers and members about exactly how your bank or credit union will communicate with them—and how you won't.

Make information about smishing part of your company's communication plan.

Provide information to your customers and members about what smishing is, how to read text messages to detect potential fraudulent behavior, and how to protect themselves, their phones, and their money from potential attacks, including what to do if they accidentally click on a link in a text message that isn't legitimate. Go through multiple scenarios of what could potentially go wrong if your company was faced with a smishing attack and consider how your company will respond.

Prepare a communications plan with planned responses to some of the most common adverse scenarios your company could face. Your company can immediately use these if you're attacked; if needed, pivot your response and communication in real time.

Use a third-party service, such as PhishLabs, that will notify your organization about potential smishing-related attacks.

What to do if your bank or credit union is attacked

- Let your customers and members know that your company has been attacked and what you're doing to address the situation and protect them. Also, let them know what to do to prevent being affected.
- Add information and a form to your website to let people know that you're aware of the attack, and provide them with a way to upload screenshots of fraudulent messages to your company.
- Report the smishing number to the FCC, Phishlabs, etc., so that the number will be blacklisted.
- If necessary, contact your state's Attorney General and bank or credit union association so they can help educate the public and media about the attack. Provide any information they need to be aware of.

Greater Nevada Credit Union recently faced challenges when its own credit union and members were the target of a smishing attack. To learn more about what happened, how Greater Nevada CU responded to the attack, and the lessons it learned from dealing with it, watch Digital Onboarding's webinar, "Manage fraud risk & reap the benefits of SMS text messaging."

ADDITIONAL RESOURCES

- Greater Nevada Credit Union Uses "Smishy" the Digital Pirate Character to Educate People About Money Scams
- "Four Tips About Smishing"

Conclusion

If you're not already texting your customers and members, doing so may seem overwhelming to your bank or credit union. But it's simply another communication channel to employ, much like email and social media. When it's used properly and you have a communications and risk plan in place, text messaging can be a highly effective and rewarding communication channel that helps improve your customer experience.

Request a demo of the Digital Onboarding adoption platform to learn how it can help you open a new line of communication and start text messaging customers and members.

See the platform in action.

Our demos are customized to fit your specific business needs.

Book a demo (267) 422-5292 sales@digitalonboarding.com

ABOUT DIGITAL ONBOARDING

The Digital Onboarding adoption platform helps banks and credit unions turn account openers into fully engaged and profitable relationships. With personalized messages, microsites, and self-service enrollment widgets and tools, the platform makes it easy for people and businesses to adopt account-related services and additional products. To learn more, visit https://www.digitalonboarding.com.