PAYMODE

A Vendor Guide to Avoiding Payment Fraud

70%

of businesses say they're concerned with fraud, either insider or external[1]

Built for Your Needs

You often see references to payers being victims when business-to-business payment fraud occurs. That's understandable, given that they have been duped into sending a payment to a bad actor, or have a payment intercepted en route to a legitimate business.

Vendors are often overlooked in those discussions, but in truth, the impact is often even more severe for those on the receiving end of those payments that never show up. Business email compromise losses alone in 2022 tallied up to $2.7 billion in the United States, and that's money that legitimate businesses aren't able to use to grow, thrive, or simply survive in tough economic circumstances.

Because so much of the payment fraud discourse focuses on how payers can protect themselves, vendors can feel left out in the cold. This guide will improve your outlook and security by offering common sense tips for preventing fraud, advice that can help ensure your business doesn't suffer the financial and reputational losses that fraudsters so desperately want to inflict on you.

1. Payments Barometer, 2022
bottomline.com

Tip #1

Know Who (And What) You're Up Against

Fraudsters are just like us: Looking for ways to do more work with less energy. Your business will not be the sole focus for a bad actor looking to steal funds, but one of dozens or even hundreds of targets. That means a swindler is likely to use automation software, mass emailing, and other tools to send messages to businesses like yours, hoping just one will take the bait.

They typically won't know specifics about your business, though, which can help you identify them. Look for unfamiliar or flat-out wrong phrases, stilted or formal language, and an unusual sense of urgency paired with an out of the ordinary request to spot scammers at work.

Remember:

Fraudsters thrive on making you feel panicked (which motivates you to click a link or surrender information that can help them defraud your business). They don't necessarily research the businesses they're targeting and mimic their targets, however.

Actionable Fraud Avoidance Tips

Always ask follow-up questions and be wary of urgency

If your CFO (Chief Financial Officer) really does want you to change bank account details, a quick message clarifying the ask won't be a problem. If it's not your CFO, a bad actor is unlikely to be able to answer pointed questions about the why and the when.

Never click a link if you're not sure of its providence

How often do your colleagues send you a link to enter sensitive account data? If it feels suspicious, it is less risky to ignore the email or report it to your internal security team.

Tune in to tone

You know your coworkers, at least in passing, and you should be able to spot an abrupt shift in tone, spelling, and language. If it doesn't sound like Tim in Accounting, it's best to pick up the phone or use your in-house messaging tool to see if it is Tim in Accounting.

Tip #2

Safeguard Your Emails

Business email compromise and phishing are probably familiar terms, since they're common fraud schemes affecting businesses like yours. They involve fraudsters trying to get you to click a link and give up account information so they can eventually steal your hard-earned payments from customers.

As alluded to in the high-level tips on the previous page, there will be a sense of urgency with any message you get. A grifter will want to direct you to a page that looks like a legitimate login page for your bank, your payments provider, and so forth, but is in fact a spoofed page that will collect whatever fields you enter. After you put in your username and password, the fraudster will have them, and you'll be re-directed to the actual login page without suspecting that your account information was stolen.

While being aware of this kind of fraud and the kinds of tactics fraudsters use is key to avoiding the scheme, an even smarter play is securing your email by taking the human element out of detection.

Fraud losses were up

80%

last year[2]

Keep Your Email Fraud-Free

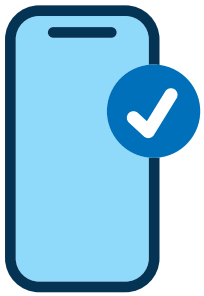
Add multi-factor authentication (MFA) for all accounts

This may seem like a hassle when you must enter a code from a mobile phone on every login attempt, but it's a life saver if someone on your team accidentally gives away their email and password. As an added bonus, the code being sent to a staffer's phone will alert you that a fraud attempt is ongoing, offering you an opportunity to change passwords and lock a fraudster out.

Let customers know you'll never request a bank change via email

A fraudster who has one of your business logins will immediately try to defraud your customers by getting them to update your bank account information for your business. Once they do, your next payment from that customer is going to enrich the wrong person. Ensure your customers know you'll always call and identify yourself if you need to make a change.

2. FBI IC3 Report, 2023



Tip #3

Protect Your Phone

If your best defense against email fraud is the phone in your pocket, the natural next question concerns whether fraudsters will go after that phone. Unfortunately, the answer is a resounding yes.

A bad actor with access to your phone (or at least your phone number and contacts) can wreak havoc, given how easily a code sent to your phone number can defeat MFA challenges. An increasingly common fraud scheme involves a bad actor who identifies your phone number calling up your carrier or accessing your account in an online portal, pretending to have lost a phone, and asking them to switch your number to their SIM Subscriber Identity Module (SIM) card. Once that happens, you're in trouble.

Fortunately, it's simple to protect your phone by securing it via multi-factor authentication and placing a Personal Identification Number (PIN) on your SIM card. In combination, these two measures can virtually ensure you lock swindlers out of your device.

Shut Down Phone Fraud Attempts

Log in to your cell phone carrier's portal and ensure you have MFA set up for your account to help protect it from fraudsters

Then navigate to your SIM card security options and set up a four-digit PIN code that must be entered to switch your number to another SIM card. As a side note, be sure to write down your PIN, as you can lock yourself out of your phone entirely if you forget it.

While you're at it, take steps to protect any business phones from similar attempts

Log in to your company's Voice Over Internet Protocol (VoIP) portal and set up MFA challenges for any access to your account there. Be sure to send those challenges to your newly secured cell phone. That way, you can not only reject any fraudulent attempts to log in, but also know whenever someone tries to access your business phones.

Finally, make sure everyone else in your organization takes similar steps so there are no weak links that bad actors can exploit

Tip #4

Switch to Secure Electronic Payments

Checks may be slow, but they were once relatively secure, so it was easy for businesses like yours to tolerate delays in the service of not having payments intercepted. Unfortunately, those days are done.

With fraudsters finding sophisticated ways to swipe checks and re-direct payments to their accounts, that payment method should be phased out as soon as possible.

The solution is to embrace—and with payers who aren't using a payment solution, encourage—the use of payment networks. Bottomline's Paymode is an example of one such network where **over $450 billion in payments are exchanged annually without fraud,** which is a direct result of the care taken to authenticate every business on the network and monitor transactions for signs of fraud.

Whether you choose Bottomline or another provider, just ensure that the ACH and virtual card payments you're accepting are coming through a solution provider who prioritizes security and has a strong track record of preventing payments fraud. If it's not secure or it doesn't feel secure, that merits a conversation with your payer, since it's your money that's ultimately at risk.

62% of businesses believe real-time payments will increase the risk of fraud[3]

Tip #5

Be Ready For Future Fraud

The only sure thing in life and fraud alike is that change is inevitable. The methods grifters are using today to try to access your phone and your email to swipe your hard-earned payments will evolve as businesses get better at protecting themselves. That means you can't set and forget your fraud prevention efforts.

Be sure to subscribe to industry publications, governmental fraud alerts, and technology newsletters to keep your knowledge of fraud sharp. While you're doing that, keep an eye out for these evolving fraud methods, which may become more major concerns soon.

3. Strategic Treasurer, 2023

What's Next for Fraud?

AI creating more effective messaging

Fraudsters may be dealing with language barriers or a lack of familiarity with your business and your customers now, which can trip up their best efforts. While artificial intelligence is still very much a work in progress, it may someday be good enough to help fraudsters adapt their messages to sound more authentic and more convincing. Keep your fundamental wariness of urgent-sounding emails in mind at all times, because the asks you get today may not be the ones you get a year from now.

Beware synthetic identities

The fastest-rising kind of fraud, synthetic identities are dangerous for consumers and businesses because it uses bits and pieces of a person's actual identity (usually a Social Security Number) combined with fictional elements to create something compelling enough to open bank accounts and pry open other accounts. While this isn't a major concern in the B2B space just yet, it may become one as bad actors figure out how to apply their efforts to defrauding companies.

Real-time payments

We're still years away from real-time payments taking off in the B2B space, but once they do, you can bet that swindlers will be swiftly developing new ways to take advantage of the technology. If your business gets the opportunity to roll out real-time payments, be sure to take a step back and find vulnerabilities before you make your major investment.

Enjoy Peace Of Mind

By bearing these five tips in mind and implementing the commonsense protections in this eBook, you can protect your business, your payments, and your customers against the best attempts of fraudsters. That's well worth the time and energy.

Want to learn more about being paid securely through Bottomline's Paymode?

GET STARTED

Bottomline

REV US021325KH