How I almost got scammed

(Recorded on 26 June 2026)

Introduction

Lucile Rives: A while ago, I was having dinner with a group of friends. My friend Andrea told us she'd recently been scammed by someone pretending to be her from her bank.

Andrea: I was completely taken in. The scammer pretended to be a bank adviser and managed to get me out of my house in a matter of minutes, on my bike. I have to admit, looking back, that it was really well done.

Lucile Rives: There were eight of us at dinner. Some knew people who'd been caught out by spectacular scams such as fake diamonds and romance fraud. Three of us had been directly targeted by scams involving fake bank advisers. Including Andrea and me.

Andrea is a lawyer and thought she was too young to be scammed. As for me; I'd just recorded a podcast episode where the Director of Financial Education at the Banque of France explained:

Marguerite Collignan: To pull off their scams, fraudsters play on people's fears. With younger people, their exploit their belief that they can get rich without taking any risks. With the elderly, they create a sense of urgency and trigger strong emotional reactions. But people in the middle age groups can also be victims of fraud.

Lucile Rives: The point is that scams are extremely sophisticated. Even if you think you're well informed, you can still get caught out. I'm going to share our experiences with you in the hope that you never come across a fake delivery driver, a fake bank adviser, a fake Brad Pitt or a fake diamond dealer. But if you ever do, I hope something from this episode sets off a little alarm bell in your mind and helps you avoid falling into the trap.

My name is Lucile and I work at the Banque de France. Welcome to L'Éco en court.

The facts

Lucile Rives: I was expecting a package. I'd arranged to be in when it arrived, but it still hadn't turned up so I popped out to do some shopping, pick up the kids at school, that sort of thing. I'd just got back when I got this message:

Delivery driver: Hello, this is your delivery driver. I came by 30 minutes ago to drop off your package. It was too big for your letterbox, so I've sent you a text message to arrange a new delivery date.

Lucile Rives: I was a bit annoyed that I'd missed the delivery. So, as I was putting the shopping away and helping the kids with their homework, I clicked on the link sent with the voicemail to reschedule.

Did I think it was odd that I had to pay 47 cents for a second delivery? Yes and no. Yes, because I'd never been charged for it before, and no because it seemed reasonable, as the delivery driver would have to make a second trip. So I gave them everything they asked for: name, address and, of course, my bank card details.

It wasn't until a few days later, when I received the same message again, even though I'd finally received the package, that I started to suspect something. Just to be safe, I cancelled my bank card and then forgot all about it. But the scammers were just getting started.

Lucile Rives: A week later, I got a phone call. The man on the line sounded calm and concerned. He introduced himself as a member of the fraud prevention team at my bank. He was reassuring but also warned me that, yes, my bank card had been cancelled, but unfortunately not quickly enough. A EUR 600 payment to Abidjan was pending on my account. My friend Andrea got a similar call. In her case there was a EUR 500 payment to Algeria that was supposed to go through.

I told Pierre Bienvenu, Head of the Retail Payments Division at the Banque de France, what had happened.

Pierre Bienvenu: Fraud really can affect anyone, including people who think they're well aware of the risks. There's a common perception that scammers mainly target older people. In reality, figures from the French Ministry of the Interior show that the biggest victims of financial scams are those aged 25 to 49, in other words, working-age adults. Fraud affects all age groups and all social and professional backgrounds. But the 25 to 49 age bracket is particularly vulnerable. These are people who tend to have some savings or assets and often lead very busy lives, creating opportunities that fraudsters are quick to exploit. People like you, Lucile. You're exactly the kind of person they're looking for.

Lucile Rives: Our fake fraud-prevention officers were also trying to help us, as well as scam us. In my friend Andrea's case, the fake adviser was very proactive. As a precaution, he told her: "We'll cancel the card, but don't worry, you'll still be able to pay with your phone. We'll only cancel the card for online payments."

Andrea: I was immediately reassured. These things are really well done; the card was only blocked online.

Pierre Bienvenu: Scammers pretend to be someone you can trust, who will help you manage your busy life. People really appreciate that. Victims like feeling supported, helped. That makes them lower their guard.

Lucile Rives: Exactly. Our fake fraud prevention officers had to earn our trust because they needed us to cooperate to be able to scam us. They needed us to give them our code. So they told us to get to a bank branch as quickly as possible. I thought that was strange, and something just clicked in my mind, and I decided to hang up and call my real bank adviser. He confirmed that my card had been cancelled, that there were no suspicious payments pending and that no fraudulent transactions had gone through my account.

Pierre Bienvenu: The anti-fraud systems did exactly what they were supposed to do. You gave away your card number, and the card has since been cancelled, but the fraudsters couldn't do anything with the card number alone. Because these days, for online payments at least, strong customer authentication is required. The fraudsters needed you to do one more thing: approve the transaction. That's why giving someone your card number is no longer, or at least not always, enough to make a payment, although it's clearly not a good idea. That's a good thing.

Lucile Rives: Unfortunately, my friend Andrea didn't think to hang up. So, still with the unwavering support of her fake adviser, a real conman, she went off to find her nearest bank branch to give him the strong authentication code he needed.

Andrea: He said: "We'll carry out a transaction together to stop any money being taken out of your account. You need to go to your bank branch to confirm that you're in France and that you're not the one making the withdrawal in Algeria. How soon can you get there? "

Lucile Rives: She went to a first branch, and the cash machines weren't working.

He called her back when she was in front of the machine, the one that wasn't working.

Andrea: I asked him: "So what do we do now?" I genuinely felt like we were partners, that we were trying to solve the problem together.

Lucile Rives: The trap had already been sprung. She went to a second branch.

Andrea: I was rushing headlong into the trap. But the branch was closed.

Lucile Rives: With this sense of urgency, of working as a team, the scammer didn't even have to tell her to find another branch. She just went ahead.

Andrea: He said: "Here's what you need to do to get a withdrawal code remotely, by text message."

Pierre Bienvenu: These are criminal organisations that gather information on the banking processes and security procedures used by different banks, so they know exactly how to guide customers step by step, whichever bank they use. They're very cunning. They use reassuring and supportive language, but they also know exactly what you have to do on your banking app, which immediately puts the customer at ease.

Andrea: He said: "The last step is to authorise the withdrawal, but nothing will be taken out of your account, it's fine." That's when I started to laugh. I said: "How do I know you're not a scammer? Prove that you're not a scammer. I really don't want to be scammed. My friends will still be laughing about it when I'm 80. Here's the code, no problem, thanks for your help."

Lucile Rives: The fastest ever bike ride across Paris and EUR 500 down the drain, and Andrea was left wondering what on earth happened.

Who pays?

Lucile Rives: As well as leaving you feeling terrible that you were scammed or almost scammed, this kind of carelessness also comes at a cost.

Pierre Bienvenu: That brings us to the sensitive issue of fees. The general principle in payment fraud cases is that, unless the customer has been grossly negligent – and that's the rub – the bank has to reimburse all fraudulent payments made on the account. If the transactions have been debited without you providing strong customer authentication, they're automatically reimbursed. If you provided strong authentication, banks are required to analyse the specific circumstances of the transactions, and the way the strong authentication was obtained. The transactions are dealt with on a case-by-case basis, and in each case the bank has to decide whether there was gross negligence. If it decides that you were grossly negligent, it won't reimburse you. But you can contest the decision by filing a complaint or referring the matter to banking ombudsman. As a final step, you can also take legal action to establish whether there was gross negligence on your part.

What can you do to prevent fraud, or at least limit the damage?

Lucile Rives: First, you need to stay alert and remember that personal data is precious. Never share your strong authentication codes and only enter your bank card details on trusted websites.

It's also worth remembering that a bank does not need your help to block a transaction. If it thinks a transaction is too risky, it can decide to reject it. And a bank will never ask you for your codes. It's also highly unlikely that your bank adviser will phone you from a number starting with 06 or 07.

Remember also that there is never any urgency. Always take the time to verify the identity of a caller or the recipient of a bank transfer. If in doubt, don't hesitate to call the person concerned or your bank adviser.

You can also report fraudulent text messages by forwarding them to 33700. This reporting services is managed by French mobile phone operators. Based on the reports they receive, they can investigate whether a number is being used in accordance with their terms and conditions and disconnect it if necessary.

Lastly, if you think you've been a victim of a bank card scam, cancel your card immediately.

Pierre Bienvenu: You absolutely did the right thing by cancelling your card. It means you're starting with a clean slate and that your card number, which is now on the dark web, can't be used to make payments.

How worried should we be?

Lucile Rives: We keep hearing about highly sophisticated scams, stolen data that can be sold on the dark web, a wide range of potential targets and victims. The list goes on. how worried should we be?

Pierre Bienvenu: It's definitely worrying, but if you look at the actual figures, especially for bank card fraud, they've been going down for several years, and they're still falling. Card payment security has been strengthened considerably, thanks both to strong customer authentication and measures introduced across the payments ecosystem. Artificial intelligence tools are also being used to check whether transactions are consistent.

Lucile Rives: Whatever the case, we need to stay vigilant. Thanks to everyone for listening. And special thanks to Pierre Bienvenu and Andrea for contributing to this episode. If you enjoyed it, please share it and leave us your comments and stars. Till next time!