Customer Fraud and Protection

Transcript

Brooke Szymik

Hello, everybody, and welcome to the Student Loans Company Customer Compliance: Mitigating Student Fraud presentation. My name is Brooke Szymik, and I'm an investigator within the Customer Compliance department. So, we have 45 minutes for this presentation. My expectation is that it'll take around 30 minutes for the presentation, and then there's an opportunity for you to ask any questions at the end of the presentation.

There may be some information that I am unable to give, due to operational security processes and due to the sensitive nature of the work that we do. Some information can't be released in a public forum, but if that's the case, I'll notify you of that in my response. So, the structure of the session, I'm going to run through the structure of what this presentation will entail and the sections that we'll be covering.

And again, to highlight, at the end of the session, if you have any questions, feel free to raise them at that point. If you do have any questions in the room, if you could raise your hand and my colleague will bring you a microphone, and if you have any questions, you can submit them through the app and I will deal with them at the end of the session as well. I hope that you find this all interesting and that it gives you some insight into customer compliance as you are in your role as education providers.

So, within this session, I'll be covering customer compliance. So, what we do, the investigation process or how we investigate, what case types we investigate. I'll cover a bit about quality assurance and investigation integrity, and that's basically ensuring how our decisions are correct and the sanctions that we apply. We realise that they can have serious consequences for students and education providers.

So, it's important that all of our decisions are correct and consistent and that the investigation work is performed professionally and to a high standard of quality. I'm going to cover a bit about social engineering - what is social engineering, how it affects students and what the SLC are doing to mitigate this type of fraud. And then finally, I'll wrap up with a summary and obviously you'll have your opportunity to ask any questions at that point.

So, what we do. I'm just going to tell you a little bit about our statement of intent. Now, it is available on the gov.uk website, at SLC Customer Compliance Statement of Intent. But to summarise, we basically have a responsibility to pay the right amount of support to the right people at the right time and to ensure the correct repayment of loan balances.

We're committed to the detection and prevention of errors and fraud in the student finance system. So, customer compliance, what we do, we carry out investigations. Now, we can get those from either internal processes or from third party referrals. And where fraud or error is suspected with students from England and Wales, we would investigate those referrals.

For students studying in Scotland and Northern Ireland, we work in conjunction with the Student Awards Agency Scotland and the EANI respectively to take appropriate action to detect and prevent fraud within the full student finance system. We conduct analysis and verification of information to ensure that our assessment process continues to operate efficiently and effectively and to identify organisational risk and proactively identify fraudulent activity.

So, they're the core components of our compliance and risk management strategies and our function is assessed annually against the Government's counter-fraud functional standards. So, we do recognise that obviously, not all mistakes on applications are fraudulent and we want the SLC experience of a student applying for funding to be as straightforward and clear as possible.

And when we do recognise that on occasion, incorrect information can be entered, it may still trigger the need for an investigation to be conducted. We still need to verify the information that's given relating to a student's eligibility to ensure that they're receiving the correct level of funding. We can go out to publicly available sources and to third parties to verify this information.

Evidence of a customer's identity, their residency and eligibility information may be collected from third parties and other government departments and from, again, publicly available sources of information. A customer's application would only be deemed fraudulent where there's sufficient evidence to make that determination.

And throughout this presentation, you'll have the opportunity to learn how we ensure that students within the customer compliance process are treated impartially, in a fair manner, and how we ensure that any decisions that we conclude are just and proportionate. So, in relation to sanctions - where an application for student funding is deemed to be fraudulent, sanctions may be applied. Now, the sanction is determined, obviously, based on the level of the fraudulent activity within the application.

A range of sanctions can be applied and these can range from a warning which is given to the student to advise that if similar conduct is found in future, then that may result in the removal of funding. We can immediately recover any payments which have already been made to the student. We can terminate a student's full eligibility or some elements of their funding.

That can be backdated to the start of the academic year and prior academic years. We can also pass the student's details to the UK's national fraud database, and that can have a detrimental impact on the student's ability to obtain credit in the future. And we can also refer to the law enforcement and prosecuting authorities.

And again, I'll reiterate that sanctions are only imposed when we have sufficient evidence to, based on each individual case, to obviously confirm the extent and the severity of the fraud, and everything, all the different elements are taken into consideration. So, I'll explain that a bit further in the decision-making process. And this is just a little bit of information about how we identify cases for review. So, we have standard referrals that come to us. We also have campaign work. So, within our standard referrals, these are identified as small group cases or individual cases.

They can come to us from within the SLC function, such as the assessing teams reviewing the application and flagging up that they have suspicions. The contact centre can pass over for referrals. Our formal appeals function and complaints department, they can also send over applications for review. We have a whistle-blowing line where people can anonymously provide information that they obviously deem to be worth investigation.

And then we have external reports from agencies and obviously education providers where they may be providing us with information where they deem that there's fraudulent activity going on. All of these referrals that we receive, we will review and determine if there is sufficient evidence for us to take on as a case.

For our campaign work - these are larger volume cases. These are usually grouped together due to shared characteristics. So, we receive that work by our analysts, they analyse the data, identifying high-risk groups. They then pass the data on, and that is reviewed by the QA and Campaigns team. They will obviously take a look through all of the information to ensure that it's accurate and it is worth review.

The Campaign team then produce the guidance material, and the guidance material is then reviewed by management. And then, they pass all of the cases over to the investigation teams who would then conduct the cases on an individual basis. However, looking at the large group with all of the information that's collated once it's received.

So, the investigation process - we're just going to move on and learn about what our investigation process looks like. So, when we as investigators are passed a case for review, we will, first of all, conduct our initial checks. From the initial checks, we will then decide if that case can be closed, there's no fraud concerns, if we believe that there's nothing to investigate.

Or we will then go out and request evidence from the student. As education providers, that's the first point that the student is aware that they're under investigation. Once the student has provided the evidence to us, we will then review the evidence. We will perform any additional checks, if any of the evidence needs to be sent out to third parties to be verified. We will then progress to an interview with the student.

Again, this is another point where education providers can be of use to the student if they're particularly nervous about an interview or if they need a bit of assistance with that. Once the investigation has had the interview concluded, we would then, in some cases, we may ask for additional evidence. If not, we would then produce a decision which would be sent to our second-tier department.

The second-tier department would then review the decision and provide clarification for the provisional decision letter to be issued. The provisional decision is sent to the student. That then gives them 21 days to provide any additional evidence, and then they are given the final decision. So, the evidence request phase - as I said, that is the first point that the student is aware that there's an investigation going on. It is the first time that they might seek assistance from yourselves, you know, to help them with the process.

It's at that point that we would also go out to yourselves as education providers and request any information that we need from you. And we do that under, obviously, a DPA or GDPR request. The type of investigation... the type of evidence that we would request would be based upon the investigation that we're conducting. And each evidence request is tailored to that particular investigation.

When a student signs the terms and conditions, they agree to provide information we require in order to support the application for funding, and that is how we are able to request additional evidence from them. And the interview phase. This is another point where the students may request assistance from you. This is just to clarify that obviously, we're aware that as a student's being interviewed, it may cause them some worry.

But we conduct our interview to the highest standards following the PEACE models and in line with best practice. They're not meant to be... interrogatory or forceful, but we do need to obviously ask them the questions that we need the answers to.

All of our interviews are conducted in line with the PEACE model. So, a little bit about what we investigate. As you can see, there's a lot of different areas within the student finance application process and there's lots of different elements of support that we can review. I'm not going to go over all of them, you can have a little read through yourself, but... we have a lot of varied types of investigation, and that is why when a student is requested evidence, this evidence isn't always the same evidence that we would request of every student.

It's tailored based on what we're investigating. I'm just going to give you a little bit of information on some of the investigations that we've performed. So, the childcare grant - previously, obviously, the childcare grant was paid to the students.

Now, since 2021, it's been paid through the Wider Plan system and the childcare grant is now paid directly to the childcare provider. It has reduced the opportunistic fraud element, but we do still see fraud coming through. An example of a case of this would be where the childcare provider was receiving funds for providing childcare to a child who wasn't actually in attendance, and they were advising that they were paying £200 a week to a child who hadn't attended for potentially over six months.

Obviously, in a real-life scenario, we wouldn't, if it was coming out of our own pocket, you wouldn't expect to be paying that high level of funding when you weren't receiving a service. So that was taken on for investigation....and obviously we deemed that the childcare hadn't taken place. Migrant workers.

So, in order to be eligible for student finance, if the student qualifies as a migrant worker, they have to maintain that employment through the time that they're in study. Now, we have detected and prevented fraud where a wide range of false employment evidence has been submitted. This can include wage slips, bank statements, employment contract, self-employment evidence, business bank accounts. All of these documents can be provided as false and therefore the employment isn't genuine and it isn't effective.

And a recent example of this, where a student's provided evidence that they were working with a taxi firm - they provided their employment contract, wage slips, bank statements showing their employment income. But we were able to confirm through contact with the taxi firm and other methods that the student wasn't employed and that the documents provided were false. The student in this case was deemed ineligible for the submission of false documents and for their eligibility to support.

They were added to Cifas for a period of six years. And now, organised fraud. This would usually involve a criminal group working together to make multiple applications for student finance, for funding that they're not entitled to. Organised fraud, it could be a criminal group using stolen identities or paying people to use their identities.

They could use people and advise that they're intending to study, but then take the money from them. Organised fraud often attempt large scale false document submissions as well. In all cases where we were able to detect and prevent organised fraud, we do so using various methods employed by our analyst team and through the wider business. Where organised fraud is suspected, we will open a campaign and all applications would be reviewed as part of that campaign.

Organised fraud and campaign cases can often request a high volume of evidence. This is so that we obviously verify that all the information given on the application is correct and it's accurate and we can obviously make the links to determine if this fraud is organised.

So, this is a bit about our decision-making process and how we ensure that the investigation that we perform is correct and we ensure that all of our students are treated equally and fairly. So, we have a consequences model. And as part of a decision-making process, the investigator must apply a score to the case when it is sent up for the provisional and final decisions to be made.

So, all of our cases are scored using the consequences model to ensure that we have consistency and fairness across all cases. So, the initial score is applied depending on the severity of the fraud being investigated. And then we would apply either mitigating or aggravating factors to obviously higher or lower the score.

So, an example of aggravating factors, for instance, would be length of fraud or if the student had previously already been warned about their conduct, and an example of mitigating factors, that could include the student obviously admitting what they'd done, or if they hadn't gained financially as a result of the information that had been given. As I said, the use of the consequences model ensures that our decisions are fair and accurate and consistent.

So, our second-tier review team, they review all decisions where a sanction has been made or if a non-response decision is applied. A student would go to non-responsive, basically, they hadn't responded to any of our requests for evidence. Now, a wide range of factors are considered in determining the appropriate sanction on an individual case-by-case basis. Having regard to the extent and the severity of the fraud and obviously ensuring that there's consistency in the decision-making process.

All sanctions go through a QA process so that we can be confident that our decisions are accurate. All students have the right to appeal our sanction decision once they're made finalised, and if these decisions weren't found to be fair, they could be overturned on appeal. Obviously, second tier help to provide a fresh, independent set of eyes on a case where an investigator has performed the investigation.

The second-tier department don't perform investigations. They oversee the investigation and review all of, obviously, the investigation process that we've been through. Investigations can take a significant amount of time and sanctions can have serious consequences for the students. And that can obviously lead to complaints about our department, if they weren't done in a fair and consistent manner.

And we follow a quality assurance framework. So, our QA team, they perform regular quality checks on all work performed to ensure that it's a high standard. That involves the investigation process to ensure that that is consistent across all investigations.

It includes the calls that we handle with students - again, the interview process, making sure that we're following in line with the PEACE model, inbound telephone calls from students, making sure they're all handled professionally and all correspondence that's sent out to students as well is quality checked. So, I'm going to move on to social engineering. And I'd just like to quickly ask anyone in the audience if they've ever received a phishing email. Yeah? So...

According to the National Crime Agency, fraud is the most commonly experienced crime in the UK. It's also been widely reported that cybercrime has soared through the pandemic. Now, data breaches continue to be a key enabler of fraud. Information is power. Personal and financial information obtained in a data breach can be used to commit fraud against individuals in the private and the public sectors. And by harvesting this information, criminals are able to commit fraud and damage people, businesses and services.

So, we're going to discuss social engineering now, which is a cybercrime that criminals use to manipulate and to trick people into giving out their personal information. It could be downloading software, sending them money. I know I've had experience of this before, and these scams can be elaborate and highly convincing, and it's a type of fraud that can affect everyone.

So, some of the scams that fraudsters use is phishing and vishing. So, these are the two types of scams that criminals use to try to gain your information. For student finance, they could ask you to sign into your online account, following a link. Phishing is an activity that's designed to trick you into giving out your personal information.

Phishing is done over the phone, so where someone can call up and impersonate you, trying to gain access to your information and to your online account. Now, baiting is similar to phishing, but it plays on fear and intrigue. It's slightly different from phishing in that it lures the victim with attractive offers, and it can be mainly used to install spyware or malware on your computer. And pretexting or smishing.

So, these are text messages that are used by fraudsters to create a fake identity and manipulate victims into providing their information. So how does phishing affect students? Phishing is a key tool that fraudsters use to attempt to steal students' funding every year. They target students with fake emails and SMS text messages.

Students might be unaware that they're being phished. They might think that those emails are genuine. There have been fake SFE emails that have been sent out to students. What we would advise is obviously if a student is ever suspicious of any emails that are received from the Student Loans Company, if they have any concerns at all, then they can call in or they can obviously have a look on their online account for the information if it's, for instance, asking for additional information.

So, the key dates of focus are September, January and April payment dates. Phishers in general will often try to gain access to the payments just before they're made. So that's the key dates for the students to be aware of. Customer compliance have a range of methods and fraud analytics to stop the scammers in their tracks.

But students have to be the best and first line of defence. If a student is phished, then we would contact them and they can call back through to SFE directly and they'd be passed through to our department. This next slide is just a little video on phishing. So, if you just want to watch the video. Phishing is any activity designed to trick you into giving out your personal details.

Fraudsters can then use this information to log into your online account, steal information and potentially your money. Be aware that phishing scams can happen at any time, but students are often targeted around payment dates at the start of term. Phishing emails and texts are often sent out in bulk. They seem official, but if you look closely, you'll often find they're unlikely to contain your first and last name.

Another tell-tale sign of a phishing communication is poor spelling, punctuation and grammar. Always ensure that you're using a secure website when submitting sensitive information online and don't post personal info on social media pages. If possible, avoid logging in on public networks too. Be suspicious of any urgent requests for personal or financial information.

If you believe you have received a phishing email, let us know by emailing phishing@slc.co.uk. So just to reiterate how to avoid phishing scams, keep an eye out for any emails or phone calls or SMS text messages that look suspicious, especially around the time that students are expecting payments.

These fraudsters create fake emails, fake texts from SFE, SFW, or the Student Loans Company, and they can really look like the genuine article. If you're not 100% sure, just never click on any links, report any suspicious links and contact... make sure to make contact through the official channels, as it's better to do that than to fall foul of a phisher.

We advise that students shouldn't post messages online that they're going to get their student finance payment soon, because that's like a big red flag that I'm going to get a big payment, come and try and get my details. We'd advise them to ensure that they're using a secure website when they submit their sensitive information and again, not to publicly post personal information online or on social media. If they can avoid logging in to their student finance account on public networks or computers, that would obviously assist.

And they have to be careful of who can see their screens when they're logging in. If they're in a public space, people can look at the information that they're providing. So, what the Student Loans Company is doing to help prevent phishing.

We have an analyst team who use various tools to proactively monitor the accounts that we suspect may have been phished. If bank details are changed, the student receives a text message or an email, and if they didn't do that change, then they need to contact us immediately. Fraud and scams are always changing, and so is our approach. We can't predict how often or when the attacks may happen. However, we run awareness campaigns in September to highlight the risks of phishing to students.

And obviously, as I said previously, September, January and April are always the highlight for the phishing season. We actively work to close down the sites to stop students from being caught out, and any reports of fake sites or links can be sent to our data security team to investigate. And if you get an email, or your students get an email which they think is a phishing email, they can send that to phishing@slc.co.uk

If they receive a phone call and they think that might be part of a vishing scam, they can email furtherinfo@slc.co.uk. And that would help to protect their account and their personal details. So, a real example of phishing for you. This is just to obviously show you how phishers have moved on.

So, the analysts identified suspicious changes to a student's account near a payment date. They attempted to make contact with the student. We emailed them using their original email address and attempted to make contact on the original phone number, not the details that had been changed. So, we then received a response via email confirming that they did make the changes and that they would ask for their payments to be made to the account that they provided.

We advised them that we needed a new bank account as part of our security process, so that bank account was provided in the student's name. We performed additional checks on this bank account, due to the suspicions that were provided with the bank statement, and it was verified that the bank statements had been provided that were false and they weren't in the student's name.

And the real student then actually got in contact with us and confirmed that they hadn't made any previous contact with student finance. So, it was the phisher who had been contacting us, providing all the new information and confirming everything was correct. So now, I'm just going to quickly summarise, and if you've got any questions, you'll be able to ask those.

So just to summarise, I hope that you can leave with an understanding of the purpose and the structure of Customer Compliance, an understanding of the investigation process that we go through, the different areas that we can investigate, hopefully understand how our second-tier process works within Customer Compliance, and any sanctions that Customer Compliance can apply, and have an understanding of social engineering and how this can affect students.

I invite you now to ask any questions, if you have any. And the final slide that I'm going to show you does have our contact information and my contact information, if you have any specific questions that you need to ask or any queries in the future.

Female Speaker

(INDISTINCT SPEECH)

Brooke Szymik

Can you just...

Male Speaker

Oh, sorry…

Female Speaker

When you say interviewing students, do you do that in person, or phone, or...?

Brooke Szymik

Yeah, we do that over the phone. We would contact the student by the phone. We would have an interview plan prepared and we would obviously go through the PEACE model to ensure that all of the questions that we require answers to are dealt with at that point. And after the interview, we would then either send that up for review or if there's any further information that the student wishes to submit, we would do that.

Sometimes the interview reveals that there isn't any fraud concerns as well. Any other questions? No? Well, I hope you've enjoyed the presentation. And as I said, if you do need to contact us, there's my email address and the phone number for the Customer Compliance department. Thank you for your time.

For more information:

events@slc.co.uk

www.slc.co.uk