Understanding the student loan lifecycle and fraud risks

Student loan approved → School certification → Funds disbursed → Student account credited

How does fraud happen at each phase of the application lifecycle?

Loan approved: Identity theft is the largest fraud risk in this stage and is often seen as cosigner fraud. When a student doesn't have a cosigner, they sometimes resort to purchasing cosigner information. They will either purchase the identity from the dark web or through online and social media advertisements that claim to "help" students by matching them with willing cosigners. In these situations, the student thinks they are getting information from a willing cosigner, when in reality, the information has been stolen, and the cosigner is actually a victim.

School certification: In situations where we have a question about school certification data, we may request documents to verify the identity and enrollment of the borrower. These documents are reviewed to verify their validity. Providing fake or altered documents is a common tactic used by perpetrators attempting to pass ID verification.

Funds disbursed: Most loans are disbursed directly to the school, but there are some exceptions. These mainly consist of our Bar exam loans which are direct pay to students who have recently graduated from law school and are studying to take the bar exam, and our residency and relocation loans that are to cover things like moving costs for med students completing their residency. Historically, we have seen perpetrators try to exploit these loan types since they are direct pay and can have high loan amounts. We have seen classic identity theft and synthetic identities used in these fraud cases.

Student account credited: Even after the funds have been disbursed to the school and applied towards the student's tuition, there is still a fraud risk present. At this point, the greatest risk is in refund fraud. A common tactic here is to use what is referred to as a "ghost student." This is someone who enrolls in class, may attend a few classes (or pay someone else to attend), and then withdraws. Refund or excess funds checks are sent out to the perpetrator. Another area of refund fraud is overpayments. Students may take fewer classes than originally planned and as a result, their actual tuition due is less than what they received from the loan. Most refunds are sent back to the lender, preventing any fraud risk, but there are times when the refund is issued directly to the student. This may be due to timing or dollar thresholds.

What are we doing about this?

Sallie Mae loans are backed with a fraud strategy and monitoring program which identifies potentially risky applications and requires additional steps to be taken to "clear" the application. These additional steps can include real time solutions while the applicant is submitting their application, such as additional questions only the true person would be able to answer. Additionally, a small number of manual reviews are completed by our Fraud Operations team where they use the tools available to them, including calling the applicant/cosigner to confirm they applied.

What's your role and how can you help stop fraud?

1. **Ensure your school certification process is strong and allows you to verify the identity of your student with confidence.**
   a. Combine requiring documents to verify the student with a video call. Multi-layered approaches take more effort for perpetrators and are harder to beat. Additionally, most perpetrators don't want to be seen on video so this in itself can be a good deterrent.

2. **Establish disbursement policies that flow funds between Sallie and the school whenever possible.**
   a. Avoid direct payments to students.
   b. Include a refund policy that flows money back to Sallie as opposed to paying out to the student directly.

3. **Report any suspicious trends such as:**
   a. Increases in applications unable to pass the school certification process.
   b. Increases in student withdrawals resulting in tuition refunds.
      i. Full withdrawal or a reduction is classes that results in a refund due.
   c. Any application trend that was unexpected or seems suspicious.

Remember, once funds have been disbursed, Sallie has limited insight as to how the disbursed funds are used so your partnership is crucial.

What are some red flags you should look for?

- Email addresses that don't make sense for the customer (email is a 3rd party name or has mixed letters that make no sense).
- Physical address and/or phone numbers on the application that is out of your school's normal area (community colleges).
- Applicants that are calling/inquiring often into the status of their application or refund.
- Increased and unusual incoming application volume. Frequency and timing can be indicators.
- Incoming calls from services such as WhatsApp. These are legit services, but incoming calls from them should be taken with caution.

What are some common fraud trends?

- **Cosigner fraud** occurs when a borrower uses 3rd party information without their permission as the cosigner on their loan. This can be a known 3rd party—such as a parent or grandparent—or an unknown 3rd party. In situations where an unknown 3rd party is used, this information can be found and purchased through most social media sites (Instagram, Facebook), school chat boards, as well as on the dark web.
- **Synthetic fraud** is a complex form of identity theft in which the fraudster invents a person who doesn't exist. A fraudster combines a stolen Social Security Number (SSN) and fake information, such as a false name, incorrect address, made-up date of birth, or new phone number to create a false identity.
- **Refund fraud** is when a student withdraws from school or reduces their credits by dropping a class and is therefore due a refund. In situations where refunds are sent directly to students, they can then repurpose the funds. This type of fraud can be seen with 1st party fraud which is when the true person takes out a loan with the intention of withdrawing to receive the refund, and/or 3rd party fraud where a perpetrator applies for the loan with stolen information, uses an address they have access to on the application (newly constructed home, empty homes for sale}, and then requests the refund be sent to this address where they will have it picked up without detection.

Best practices

- Increase the level of fraud awareness and education with school admissions personnel.
- Ensure you *know your customer* and take additional steps to identify students when needed.
- Combine required documents to verify the student with a video call as most perpetrators don't want to be seen on video so this can be a good deterrent.
- Require applicants to submit a selfie while holding their photo identification.
- Establish sound refund policies. These should require photo identification and mailing address verification and funds should be flowed back to Sallie as opposed to directly to the student.
- If a student or parent contacts you with a fraud claim regarding a Sallie Mae loan, **don't panic. Please refer them to our Fraud Prevention Department at 877-903-7975.** Our fraud agents are available to address fraud situations, prevent fraud losses, and assist the customer with next steps and tips on how they can protect their identity.
- If you find a potentially suspicious trend or student, please provide the details to your relationship manager. They will have the account researched. When reaching out be prepared to provide applicant details such as SSN, address, phone, and email address.

Borrow responsibly

We encourage students and families to start with savings, grants, scholarships, and federal student loans to pay for college. Students and families should evaluate all anticipated monthly loan payments, and how much the student expects to earn in the future, before considering a private student loan.

The information contained in this presentation is not comprehensive, is subject to constant change, and therefore should serve only as general, background information for further investigation and study related to the subject matter and the specific factual circumstances being considered or evaluated. Nothing in this presentation constitutes or is designed to constitute legal or financial advice.

Sallie Mae does not provide, and these materials are not meant to convey, financial, tax, or legal advice. Consult your own attorney, tax advisor, or financial advisor about your specific circumstances.