WHY QUANTRAX HAS THE BEST COMPLIANCE SOFTWARE IN THE COLLECTION INDUSTRY

Quantrax CORPORATION | RMEx Receivables Management Expert

Security and compliance - These are arguably the two most important challenges facing the US debt collection industry. With a suite of technology creations that include artificial intelligence-based collection software and a truly integrated dialer, Quantrax has strategically set its sights on software that offers systemic solutions to all of today's compliance challenges.

Are we winning? You can be the judge. This document summarizes the security and compliance features of the system. We invite the industry to share and endorse our commitment to making this one of the best technology-based industries. The battle to be compliant has to be won with actions and not words. We at Quantrax are leading that fight.

SECURITY FEATURES

Security features deal with access to features and data. Clients are aware that collection companies share resources across multiple projects. Some larger clients will insist that only designated people work their accounts. Access to data must also be restricted based on an individual's role within the company. Some states require that a collector is licensed in that state before they are allowed to work accounts that originate in that state. Information that could be used to steal identities or access financial data must be protected.

All of these requirements can be met with well-designed software. The following table presents the security features of our system.

SECURITY FEATURES	
FEATURE	**NOTES**
Access to features and information can be restricted based on role and responsibilities.	
Options accessed are documented and can be viewed by management.	
Access to clients can be allowed or restricted at the user level.	
Access to accounts could be restricted based on the consumer's state.	Used when collectors have to be licensed in specific states
Users can be forced to authenticate a consumer prior to viewing detailed account information. Information used for authentication is defined by each company.	
If an account is viewed but no "access footprint" is left on the account, the system can add a note that the account was viewed by a specific individual.	Closing the session window will also add a note.
Access to medical records and related information can be restricted by user.	
Client and patient information as well as account notes can be hidden for selected users.	E.g. Users entering returned mail do not need to view client or patient information.
Key information such as social security numbers, credit card numbers or bank account numbers can be partially masked based on a user's role.	
Key financial information and social security numbers are encrypted at rest.	Client account number can also be encrypted and masked.
Our hardware platform, the IBM i5 (formerly known as the AS/400 and iSeries) offers the highest levels of system security. This platform has been awarded a C2 rating for security.	C2 is a security standard defined by the U.S. government in the Department of Defense Trusted System Evaluation Criteria.

MANAGING SOME COMMON COMPLAINTS WITH REGARD TO DIALERS

Dialers offer great efficiency with the ability to quickly work very high volumes of phone numbers. If dialers are not properly managed, they lead to complaints and the violation of some basic rules.

A majority of the complaints about dialers relate to nuisance calls (canceling calls before the consumer is able to get the to the phone, or dead air when the call is picked up), calling outside of the permitted hours or calling cell phones if they should not be called. This section summarizes the features we have to manage these complex requirements.

COMPLIANCE FEATURES

FEATURE	NOTES
When making predictive calls, our dialer does not cancel calls.	Phone is allowed to ring for a minimum period or number of rings.
Dead air is minimized because we do not use traditional pacing methods for predictive dialing.	
Our dialer can call effectively at a 1% abandoned rate. Abandoned rate is managed by the dialer and not by supervisors as is the case with most other systems.	Abandoned rate is ratio of cancelled and dead air calls to connected calls.
To determine the allowed calling period, we can look at *all* the numbers on an account as well as the consumer's state. States with multiple time zones are handled in different ways.	
For the most conservative approach, we can look at telephone exchange and zip code to determine the best time to call.	Most conservative = Most restrictive, based on all of the available information
Toll-free numbers are considered in the calculation for allowed calling period. They can be ignored.	
Daylight savings time is factored into all calculations.	
Some states specify that IVR calls should only be placed during specified hours of the day. We allow this to be specified at the state level in addition to special times for predictive calls.	
While users can opt for the most conservative calculations (the safest approach), they can override many of the options to give themselves more flexibility.	
Since most companies have desk phones, the system can mask phone numbers when they should not be called. This will prevent a collector from calling out of time zone using a desk phone.	Numbers are protected and not displayed, along with a special message.
We have cell phone scrubbing software to identify cell phones and take user-defined action in real time. This applies to new accounts loaded into the system and information later changed or added.	
By running the ported number update, existing information is analyzed by the system and updated.	Cell phone data must be purchased.
Permission to call cell phones can be obtained and notated against the number. Predictive and preview calls can be restricted to cell phones with or without prior permission to call.	
Flexibility is available at the company and / or client level, depending on the option.	
Numbers can be defined as "Do not call numbers". They will not be called when this happens.	Defined at the company or account level.

AND THEN THERE WAS LEGISLATION FROM STATES AND CITIES

It started with clients adopting a defensive posture and instructing collection companies about how they should work their accounts. In a relatively short period, the landscape changed. New legislation was introduced by states and cities. Compliance requirements have widened quickly and can often be questioned with regard to their interpretation. We believe that it is not our responsibility to interpret the rules, but that we have to provide our clients with the technology to manage their businesses effectively, while staying within the guidelines of any legislation, regardless of how they choose to interpret those rules.

Here are several examples.

COMPLIANCE FEATURES

FEATURE	NOTES
We handle state licensing requirements. If a company does not have a license to work in certain states, accounts received for those states can be handled in many ways.	Processes are fully automated.
The system will ensure that the validation notice is sent out after an attempt or contact is made.	Users can make phone calls prior to sending the validation notice.
Calling rules (maximum "footprint calls" for a day or a given period) as well as the number of calls to individual phone numbers, types of phones (home, work, cell) or the consumer, can be defined.	
The maximum number of messages that can be left by individuals or a dialer, can be managed.	
Attempts, messages and connects can be separately counted.	
There are options to define a demand letter as an attempt, and to treat a message as a contact.	Required by some states.
Rules can be set up at the state or city level.	Zip and/or area codes can define a city.
Letters can be changed or stopped based on different states or cities.	Cities are set up as zip/area codes.
Collectors are notified when states require that you inform the consumer that calls are being recorded.	
Some states require that if a home and work number exist, the home number be attempted and the work number tried only a given number of days later. We systemically manage this rule.	Work numbers will be masked so they can not be accidentally dialed.
Third party numbers can be systemically disabled so that they are not contacted multiple times.	Each phone code must be set up in the system to indicate the type of number.
If clients insist that cell phones should not be called using a dialer, we can make sure these numbers are not called through the dialer. We have methods of counting and tracking these manual calls.	
Predictive or preview calls to cells can be stopped at the company or state level	
Predictive or preview calls (autodialer calls) to *any* number can be stopped at the state level.	Permission can also be checked
Some cities require that the details of a payment arrangement be printed on a notice.	We can print print amounts / due dates

You will see that several of these requirements are related to outgoing phone calls. The solutions we describe have been built into our integrated dialer I-Tel. They will be more difficult to implement with other dialers, and may require significant customization.